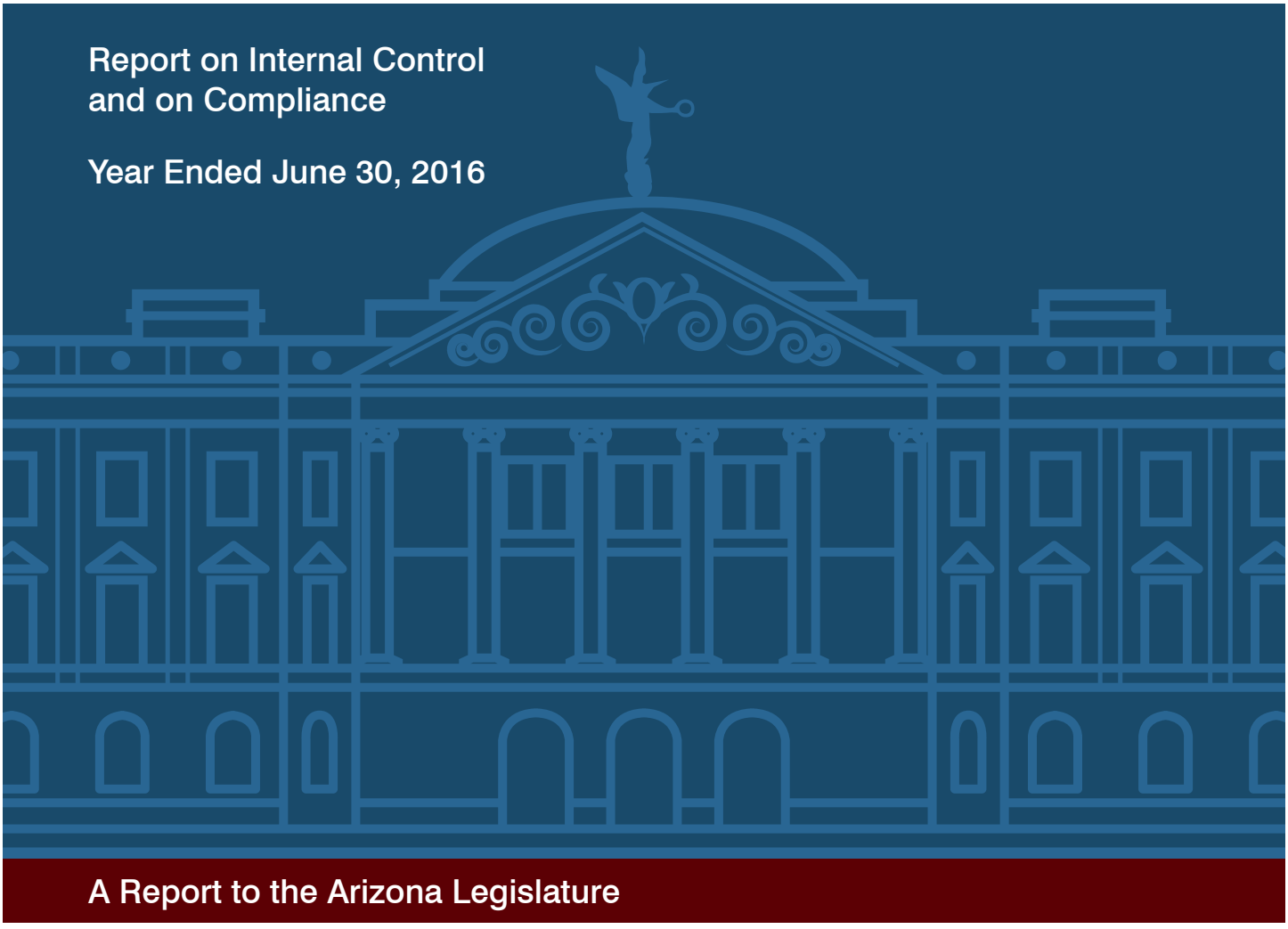
Maricopa County Community College District



Debra K. Davenport
Auditor General

ARIZONA Auditor General
Making a Positive Difference

ARIZONA Auditor General

Making a Positive Difference

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

The Joint Legislative Audit Committee

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

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

Contact Information

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

(602) 553-0333

www.azauditor.gov

TABLE OF CONTENTS

STATE OF ARIZONA
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 Board of Supervisors 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, 2016, and the related notes to the financial statements, which collectively comprise the District's basic financial statements, and have issued our report thereon dated March 16, 2017. 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 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 2016-01, 2016-02, 2016-03, 2016-04, 2016-05, and 2016-06 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 deficiencies described in the accompanying schedule of findings and recommendations as items 2016-07 and 2016-08 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 in its corrective action plan at the end of this report. The County's responses were not subjected to the auditing procedures applied in the audit of the basic financial statements, and accordingly, we express no opinion on them.

Purpose of this report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the 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

March 16, 2017

Financial statement findings

2016-01

The District should improve procedures for approving adjunct faculty employment

Criteria—The District should have effective policies and procedures requiring its campuses to perform and document supervisory approvals for all adjunct faculty employment contracts to help ensure that the District pays only for authorized and valid employment contracts.

Condition and context—The District's policies and procedures required a supervisory review and approval for all employee salaries and wages. However, the District did not always follow these policies and procedures to 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, for 35 of 60 employees tested, the employee was an adjunct faculty employee, and for 16 of 35 adjunct faculty employees tested, the District did not have sufficient evidence that the employment contract was approved. The 35 adjunct faculty employees comprised a total of 99 SIS-initiated contracts, 35 of which were 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 nearly $64 million to adjunct faculty employees during the fiscal year. Auditors were able to perform additional tests to confirm that the 35 contracts lacking evidence of supervisory approval for adjunct faculty employees were valid and correctly charged.

Cause—The District's individual colleges and skill centers did not always follow established policies, and the District lacked detailed procedures for the colleges and skill centers to follow for performing and documenting supervisory approvals of adjunct faculty employment contracts.

Recommendations—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 are consistently followed. In addition, the District should develop detailed procedures for its colleges and skill centers to follow for performing and documenting supervisory approval of adjunct faculty employment contracts and require that documented approvals be maintained either in hard copy form or electronically. Finally, the District should monitor the colleges' and skill centers' adherence to its policies and procedures over employment contracts.

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

This finding is similar to prior-year finding 2015-01.

2016-02

The District should 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 help ensure that employees are paid in a timely manner, the District's payroll system automatically approves time sheets not approved by a supervisor so payroll can be processed. The District did not have other controls in place to ensure supervisors 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 nearly $38 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 to ensure that employees' time sheets are reviewed and approved. In addition, the District should monitor the colleges' and skill centers' adherence to its policies and procedures for approving employees' time sheets.

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

This finding is similar to prior-year finding 2015-02.

2016-03

The District should strengthen oversight of its information technology controls

Criteria—A strong control environment should include a governance structure that provides oversight and requires policies and procedures that are documented, communicated to employees, and consistently applied. In addition, an effective internal control system should include monitoring of internal controls to ensure that employees are following the District's policies and procedures.

Condition and context—The District established policies over information technology (IT), had a written information security program in place, and had documented procedures for certain IT areas. However, while the District has made progress in establishing policies and procedures for many IT areas, there remain several IT areas where the District lacked documented policies and procedures. In addition, the District did not have clearly designated oversight and monitoring in place for IT internal controls to ensure that they were established and followed.

Effect—There is an increased risk that the District may not achieve its internal control objectives as they relate to the security, integrity, and availability of its information technology resources, which include its systems, network, infrastructure, and data.

Cause—The District is a complex system of colleges and skill centers, each with their own IT personnel and IT resources. Although the District has made progress in establishing policies and procedures for many IT areas, there remain IT areas that lack documented policies and procedures. In addition, while the District centralized some aspects of IT internal controls, it had not clearly designated oversight and monitoring responsibilities for its IT internal controls.

Recommendations—To help ensure that the District maintains a strong control environment and effective internal controls, the District should require and continue establishing policies and procedures for all IT areas that are documented and communicated to employees. In addition, the District should clearly designate oversight and perform monitoring for all IT internal controls to help ensure that they are in place and being followed.

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

This finding is similar to prior-year finding 2015-03.

2016-04

The District should improve its risk-assessment process related to information technology security

Criteria—The District faces risks of reporting inaccurate financial information and exposing sensitive data. An effective internal control system should include an entity-wide risk-assessment process that involves members of the District's administration and IT management to determine the risks the District faces as it seeks to achieve its objectives to report accurate financial information and protect sensitive data. An effective risk-assessment process provides the basis for developing appropriate risk responses and should include defining objectives to better identify risks and define risk tolerances and identifying, analyzing, and responding to identified risks.

Condition and context—The District's annual risk-assessment process included a district-wide information technology (IT) security risk assessment over the District's IT resources, which include its systems, network, infrastructure, and data. However, the District's risk assessment process did not document all elements of the process and its prioritization of risks identified for remediation. Also, while the District developed policies for classifying data, it did not perform a district-wide inventory of sensitive information to ensure it is protected.

Effect—There is an increased risk that the District's administration and IT management may not effectively identify, analyze, and respond to risks that may impact its IT resources.

Cause—The District was in the process of fully implementing its risk assessment process related to IT security. It had developed data classification policies, but is still in the process of developing procedures for inventorying and protecting sensitive information.

Recommendations—To help ensure that the District has effective policies and procedures to identify, analyze, and respond to risks that may impact its IT resources, the District needs to improve its entity-wide IT security risk-assessment process. The information below provides guidance and best practices to help the District achieve this objective.

- **Conduct an IT risk-assessment process at least annually—**A risk-assessment process should include the identification of risk scenarios, including the scenarios' likelihood and magnitude; documentation and dissemination of results; review by appropriate personnel; and prioritization of risks identified for remediation. An IT risk assessment could also incorporate any unremediated threats identified as part of an entity's security vulnerability scans.
- **Identify, classify, inventory, and protect sensitive information—**Security measures should be developed to identify, classify, and inventory sensitive information and protect it, such as implementing controls to prevent unauthorized access to that information. Policies and procedures should include the security categories into which information should be classified, as well as any state statutes and federal regulations that could apply, and require disclosure to affected parties if sensitive information covered by state statutes or federal regulations is compromised.

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

This finding is similar to prior-year findings 2015-03 and 2015-04.

2016-05

The District should improve security over its information technology resources

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

Condition and context—The District did not document and implement sufficient IT security policies and procedures over its IT resources.

Effect—There is an increased risk that the District may not prevent or detect the loss of confidentiality, integrity, or availability of systems and data.

Cause—The District was in the process of developing policies and procedures for IT security and had not fully implemented them and reviewed them against IT standards and best practices.

Recommendations—To help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources, the District needs to further develop its policies and procedures over IT security. The information below provides guidance and best practices to help the District achieve this objective.

- **Perform proactive logging and log monitoring**—Key user and system activity should be logged, particularly for users with administrative access privileges and remote access, along with other activities that could result in potential security incidents such as unauthorized or inappropriate access. An entity should determine what events to log, configure the system to generate the logs, and decide how often to monitor these logs for indicators of potential attacks or misuse of IT resources. Finally, activity logs should be maintained where users with administrative access privileges cannot alter them.
- **Perform IT vulnerability scans—**Policies and procedures should be implemented for vulnerability scans that includes performing vulnerability scans of IT resources on a periodic basis and utilizing tools and techniques to automate parts of the process by using standards for software flaws and improper configuration, formatting procedures to test for the presence of vulnerabilities, measuring the impact of identified vulnerabilities, and approving privileged access while scanning systems containing highly sensitive data. In addition, vulnerability scan reports and results should be analyzed and legitimate vulnerabilities remediated as appropriate, and information obtained from the vulnerability-scanning process should be shared with other departments of the entity to help eliminate similar vulnerabilities.
- **Apply patches—**Patches to IT resources should be evaluated, tested, and applied in a timely manner once the vendor makes them available.
- **Secure unsupported software**—Establish a strategy for assessing and securing any software that the manufacturer no longer updates and supports.
- **Protect sensitive or restricted data—**Restrict access to media containing data the entity, federal regulation, or state statute identifies as sensitive or restricted. Such media should be appropriately marked indicating the distribution limitations and handling criteria for data included on the media. In addition, media should be physically controlled and secured until it can be destroyed or sanitized using sanitization mechanisms with the strength and integrity consistent with the data's security classification.
- **Implement IT standards and best practices—**IT policies and procedures should be reviewed against current IT standards and best practices, updated where needed, and implemented entity-wide, as appropriate. Further, staff should be trained on IT policies and procedures.

This finding is similar to prior-year finding 2015-04.

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

2016-06

The District should improve access controls over its information technology resources

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

Condition and context—The District did not have adequate policies and procedures or consistently implement its policies and procedures to help prevent or detect unauthorized or inappropriate access to its IT resources.

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

Cause—The District was in the process of developing policies and procedures for granting and reviewing access to its IT resources and had not fully implemented them and reviewed them against IT standards and best practices.

Recommendations—To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the District needs to develop and implement effective logical and physical access policies and procedures over its IT resources. The information below provides guidance and best practices to help the District achieve this objective.

- **Review user access—**A periodic, comprehensive review should be performed of all existing employee accounts to help ensure that network and system access granted is needed and compatible with job responsibilities.
- **Remove terminated employees' access to its IT resources—**Employees' network and system access should immediately be removed upon their terminations.
- **Review contractor and other nonentity account access—**A periodic review should be performed on contractor and other nonentity accounts with access to an entity's IT resources to help ensure their access remains necessary and appropriate.
- **Review all shared accounts—**Shared network access accounts should be reviewed and eliminated or minimized when possible.
- **Manage shared accounts**—Shared accounts should be used only when appropriate and in accordance with an established policy authorizing the use of shared accounts. In addition, account credentials should be reissued on shared accounts when a group member leaves.
- **Review and monitor key activity of users—**Key activities of users and those with elevated access should be reviewed for propriety.
- **Improve network and system password policies—**Network and system password policies should be improved and ensure they address all accounts.
- **Manage employee-owned and entity-owned electronic devices connecting to the network**—The use of employee-owned and entity-owned electronic devices connecting to the network should be managed, including specifying configuration requirements and the data appropriate to access; inventorying devices; establishing controls to support wiping data; requiring security features, such as passwords, antivirus controls, file encryption, and software updates; and restricting the running of unauthorized software applications while connected to network.
- **Manage remote access**—Security controls should be utilized for all remote access. These controls should include appropriate configuration of security settings such as configuration/connections requirements and the use of encryption to protect the confidentiality and integrity of remote sessions.
- **Review data centers access**—A periodic review of physical access granted to its data centers should be performed to ensure that it continues to be needed.
- **Implement IT standards and best practices**—IT policies and procedures should be reviewed against current IT standards and best practices, updated where needed, and implemented entity-wide, as appropriate. Further, staff should be trained on IT policies and procedures.

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

This finding is similar to prior-year finding 2015-05.

2016-07

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

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

Condition and context—While the District had written policies and procedures for managing changes to its IT resources, not all changes followed the process specified by these policies. Specifically, the policies and procedures did not address all types of changes. In addition, the policies and procedures lacked certain critical elements, including ensuring changes were properly documented and tested and IT resources were configured securely.

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

Cause—The District developed change management policies and procedures in prior fiscal years in response to deficiencies found in prior audits. However, the policies were not implemented district-wide.

Recommendations—To help prevent and detect unauthorized, inappropriate, and unintended changes to its IT resources, the District needs to update its policies and procedures over its configuration management processes. The information below provides guidance and best practices to help the District achieve this objective.

- **Establish and follow change management processes**—For changes to IT resources, a change management process should be established for each type of change, including emergency changes and other changes that might not follow the normal change management process. Further, all changes should follow the applicable change management process and should be appropriately documented.
- **Review proposed changes**—Proposed changes to IT resources should be reviewed for appropriateness and justification, including consideration of the change's security impact.
- **Document changes**—Changes made to IT resources should be logged and documented and a record should be retained of all change details, including a description of the change, the departments and system(s) impacted, the individual responsible for making the change, test procedures performed and the test results, security impact analysis results, change approvals at each appropriate phase of the change management process, and a post-change review.
- **Roll back changes**—Rollback procedures should be established that include documentation necessary to back out changes that negatively impact IT resources.
- **Test**—Changes should be tested prior to implementation, including performing a security impact analysis of the change.

- **Separate responsibilities for the change management process**—Responsibilities for developing and implementing changes to IT resources should be separated from the responsibilities of authorizing, reviewing, testing, and approving changes for implementation or, if impractical, performing a post-implementation review of the change to confirm the change followed the change management process and was implemented as approved.
- **Configure IT resources appropriately and securely**—The functionality of IT resources should be limited to ensure it is performing only essential services and maintaining appropriate and secure configurations for all systems.
- **Manage software installed on employee computer workstations**—For software installed on employee computer workstations, policies and procedures should be developed to address what software is appropriate and the process for requesting, approving, installing, monitoring, and removing software on employee computer workstations.

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

This finding is similar to prior-year finding 2015-06.

2016-08

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

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

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

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

Cause—Although the District had a contingency plan and some contingency planning processes in place, its contingency plan was not updated and did not include all areas the District identified as critical in its business impact analysis and risk assessment. In addition, the District had high-level policies, but lacked detailed procedures for contingency planning.

Recommendations—To help ensure district operations continue in the event of a disaster, system or equipment failure, or other interruption, the District needs to further develop its contingency planning procedures. The information below provides guidance and best practices to help the District achieve this objective.

- **Update the contingency plan and ensure it includes all required elements to restore operations—** Contingency plans should be updated at least annually for all critical information or when changes are made to IT resources, and updates to the plan should be communicated to key personnel. The plan should include essential business functions and associated contingency requirements, including recovery objectives and restoration priorities and metrics as determined in the entity's business-impact analysis; contingency roles and responsibilities and assigned individuals with contact information; identification of critical information assets and processes for migrating to the alternative processing site; processes for eventual system recovery and reconstitution to return the IT resources to a fully operational state and ensure all transactions have been recovered; and review and approval by appropriate personnel. The contingency plan should also be coordinated with incident-handling activities and stored in a secure location, accessible to those who need to use it, and protected from unauthorized disclosure or modification.
- **Move critical operations to a separate alternative site—**Policies and procedures should be developed and documented for migrating critical IT operations to a separate alternative site for essential business functions, including putting contracts in place or equipping the alternative site to resume essential business functions, if necessary. The alternative site's information security safeguards should be equivalent to the primary site.
- **Test the contingency plan—**A process should be developed and documented to perform regularly scheduled tests of the contingency plan and document the tests performed and results. This process should include updating and testing the contingency plan at least annually or as changes necessitate, and coordinating testing with other plans of the entity such as its continuity of operations, cyber incident response, and emergency response plans. Plan testing may include actual tests, simulations, or tabletop discussions and should be comprehensive enough to evaluate whether the plan can be successfully carried out. The test results should be used to update or change the plan.
- **Train staff responsible for implementing the contingency plan—**An ongoing training schedule should be developed for staff responsible for implementing the plan that is specific to each user's assigned role and responsibilities.
- **Backup systems and data—**Establish and document policies and procedures for testing IT system software and data backups to help ensure they could be recovered if needed. Policies and procedures should require system software and data backups to be protected and stored in an alternative site with security equivalent to the primary storage site. Backups should include user-level information, system-level information, and system documentation, including security-related documentation. In addition, critical information system software and security-related information should be stored at an alternative site or in a fire-rated container.

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

This finding is similar to prior-year finding 2015-07.

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, 2017

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, 2016

Financial Statement Findings

2016-01

The District should improve procedures for approving adjunct faculty employment
Names of contact persons: Kim Granio and Sam Dosumu
Anticipated completion date: Spring 2017

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 by Fall 2016 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.

2016-02

The District should improve procedures for approving employees' time sheets
Names of contact persons: Kim Granio and Barbara Basel
Anticipated completion date: June 2017

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 as Department of Labor regulations require that employees be paid for time worked regardless of approval status. During FY2017, the District has developed and implemented a manual approval process for any time worked and paid, but not approved. Additionally, personnel policies are being reviewed to determine what progressive disciplinary action should be taken when repeated time-approver non-compliance is evidenced. 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.

2016-03

The District should strengthen oversight of its information technology controls
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 2017, and the District will refine these plans as warranted.

The District agrees. The Vice Chancellor for Information Technology and Chief Information Security Officer will work with the college presidents to achieve improved oversight.

Maricopa County Community College District
Corrective Action Plan
Year Ended June 30, 2016

2016-04

The District should improve its risk-assessment process related to information technology 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 2017, and the District will refine these plans as warranted.**

The District agrees. The District will continue to enhance and improve its Information Technology risk-assessment processes at the District Office and colleges.

2016-05

The District should improve security over its information technology resources
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 2017, and the District will refine these plans as warranted.**

The District agrees. Information technology policies, known as IT Directives, have been created, approved, and adopted district-wide to strengthen information technology security. Additional procedures will be created as needed by the colleges to further strengthen security as the threat landscape continues to evolve.

2016-06

The District should improve access controls over its information technology resources
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 2017, and the District will refine these plans as warranted.**

The District agrees. The District will continue assessing and enhancing its policies and procedures over Information Technology access controls and will continue its efforts to monitor college compliance with Information Technology policies and procedures.

Maricopa County Community College District
Corrective Action Plan
Year Ended June 30, 2016

2016-07

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

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 2017, and the District will refine these plans as warranted.**

The District agrees. The District Office Change Advisory Board (CAB), which governs the change management program and processes, meets weekly to review and communicate changes to information technology systems at the district level. CAB was further enhanced to include core members from the Colleges. The District will continue to enhance and improve its change management program and assist the colleges in updating their written guidance to reflect improved change management procedures as necessary.

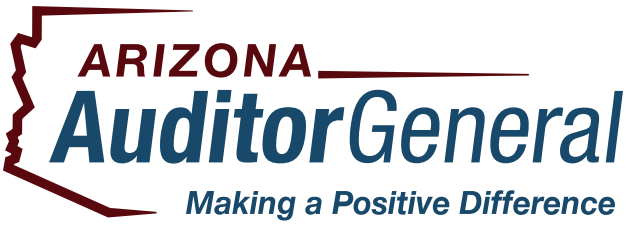
2016-08

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

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 2017, and the District will refine these plans as warranted.**

The District agrees and will continue to enhance and improve its college backup and data recovery policies and procedures.


ARIZONA
Auditor General
Making a Positive Difference