Maricopa County Community College District

Report on Internal Control and on Compliance

Year Ended June 30, 2017

A Report to the Arizona Legislature

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

Representative **Anthony Kern**, Chair

Representative **John Allen**

Representative **Rusty Bowers**

Representative **Rebecca Rios**

Representative **Athena Salman**

Representative **J.D. Mesnard** (ex officio)

Senator **Bob Worsley**, Vice Chair

Senator **Sean Bowie**

Senator **Judy Burges**

Senator **Lupe Contreras**

Senator **John Kavanagh**

Senator **Steve Yarbrough** (ex officio)

Audit Staff

Jay Zsorey, Director

Kathleen Wood, Manager and Contact Person

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

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* 1

Schedule of Findings and Recommendations 3

Financial statement findings 3

District Response

Corrective action plan

Report issued separately

Comprehensive annual financial report

STATE OF ARIZONA

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

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 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, 2017, 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 18, 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 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 have not been 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 2017-01, 2017-03, 2017-04, 2017-05, and 2017-06 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 2017-02 and 2017-07 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 in its corrective action plan at the end of this report. 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 18, 2017

SCHEDULE OF FINDINGS AND RECOMMENDATIONS

Financial statement findings

2017-01

The District should improve procedures for approving adjunct faculty employment

Criteria—The District should have effective policies and procedures requiring its colleges and skill centers to perform and record 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 did not ensure that adjunct faculty employees' employment contracts were approved. Payments to district employees are 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 before payment is processed on the payroll system. During the fiscal year, the District designed new policies and procedures to require supervisory approval of all adjunct faculty employment contracts. However, auditors examined 4 of the District's 11 colleges' implementation of these policies and procedures and noted that the District's new policies and procedures were not fully implemented at the 4 colleges examined.

Effect—The District risks paying for unauthorized or invalid employment contracts, which could potentially result in inappropriate district charges. The District paid over $52 million to adjunct faculty employees during the fiscal year.

Cause—The District's colleges did not always follow the established policies and procedures 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. Finally, the District should monitor the colleges' 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 at the end of this report.

This finding is similar to prior-year finding 2016-01.

2017-02

The District should improve procedures for approving employees' time sheets and reports

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 be performed either prior to processing payroll or within a reasonable period of time after payroll has been processed. However, the District did not always ensure these policies and procedures were followed. Specifically, for 2 of 44 employee time sheets tested, the employee's time worked was not reviewed and approved by a supervisor.

Effect—The District risks paying for unauthorized hours worked, which could potentially result in inappropriate district charges. The District paid nearly $43 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 existing procedures for approving employees' time sheets were not always followed. In November 2016, the District updated its procedures to notify supervisors of employees' time sheets that had not been reviewed and approved. The District also implemented a mechanism to follow up with the applicable supervisors to help ensure that employees' time sheets and reports are approved in a timely manner.

Recommendation—To help ensure that it pays employees only for authorized and approved hours worked, the District should require its existing procedures for reviewing and approving employees' time sheets be followed by monitoring its colleges' and skill centers' adherence to its policies and procedures for reviewing and approving employee time sheets.

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

This finding is similar to prior-year finding 2016-02.

2017-03

The District should strengthen oversight of its information technology controls

Criteria—A strong control environment should include a governance structure that provides oversight and require 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 of 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 at the end of this report.

This finding is similar to prior-year finding 2016-03.

2017-04

The District should improve its risk-assessment process to include 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 IT security risk-assessment process, such as how the various risk-assessment results were communicated to the District's administration and the District's prioritization for remediation and response to risks identified. Further, the District did not evaluate the impact disasters or other system interruptions could have on its critical IT resources.

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 fully implementing procedures for inventorying, protecting sensitive information, and regularly performing a business impact analysis.

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 district-wide IT 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 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.
- **Evaluate the impact disasters or other system interruptions could have on critical IT resources—**The evaluation should identify key business processes and prioritize the resumption of these functions within time frames acceptable to the entity in the event of contingency plan activation. Further, the results of the evaluation should be considered when developing its disaster recovery plan.

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

This finding is similar to prior-year finding 2016-04.

2017-05

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 because 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 includes 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 have sufficient written 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 but 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 IT security policies and procedures. The District should review these policies and procedures against current

IT standards and best practices and implement them district-wide, as appropriate. Further, the District should train staff on the policies and procedures. 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—**A formal process should be developed for vulnerability scans that includes performing vulnerability scans of its 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.
- **Develop and document a process for awarding IT vendor contracts—**A process should be developed and documented to ensure the consideration of IT risks, costs, benefits, and technical specifications prior to awarding IT vendor contracts. In addition, contracts should include specifications addressing the management, reliability, governance, and security of the entity's IT resources. Finally, an IT vendor's performance should be monitored to ensure conformance with vendor contracts.

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

This finding is similar to prior-year finding 2016-05.

2017-06

The District should improve access controls over its information technology resources

Criteria—Logical and physical access controls help to protect a 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 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 but 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 effective logical and physical access policies and procedures over its IT resources. The District should review these policies and procedures against current IT standards and best practices and implement them district-wide, as appropriate. Further the District should train staff on the policies and procedures. 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 the 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.

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

This finding is similar to prior-year finding 2016-06.

2017-07

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 activation of the plan; and having system and data backup policies and procedures.

Condition and context—The District did not have a written contingency plan. Also, although the District was performing system and data backups, it did not have documented policies and procedures for performing the backups or 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—The District had some contingency processes in place, but did not have a contingency plan or contingency policies and procedures in place.

Recommendations—To help ensure district operations continue in the event of a disaster, system or equipment failure, or other interruption, the District needs to develop and document its contingency planning procedures. The District should review its contingency planning procedures against current IT standards and best practices and implement them district-wide, as appropriate. The information below provides guidance and best practices to help the District achieve this objective.

- **Develop and implement a contingency plan**—A contingency plan should be developed and implemented and include essential business functions and associated contingency requirements; 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 table

top 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 at the end of this report.

This finding is similar to prior-year finding 2016-08.

DISTRICT RESPONSE

MARICOPA
COMMUNITY COLLEGES

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

February 14, 2018

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, 2017

Financial Statement Findings

2017-01

The District should improve procedures for approving adjunct faculty employment
Names of contact persons: Kim Granio and Sam Dosumu
Anticipated completion date: June 2018

The District agrees with the finding and recommendation. In February 2018, the District is implementing changes to its enterprise systems (Human Capital Management System-HCM and Student Information System-SIS) to require electronic approvals of adjunct faculty assignments initiated in SIS prior to the faculty member receiving access to his/her class roster, gradebook, etc. It is expected that these changes will provide the required improvements.

2017-02

The District should improve procedures for approving employees' time sheets and reports
Names of contact persons: Kim Granio and Barbara Basel
Anticipated completion date: June 2018

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 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. Finally, with the changes to the District's Human Capital Management (HCM) system in February 2018, the approval process is significantly easier for supervisors to execute; therefore, increased compliance is anticipated.

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 are investigated. Furthermore, project directors manually certify all grant-funded time sheets not approved by a supervisor.

2017-03

The District should strengthen oversight of its information technology controls
Names of contact persons: Edward Kelty
Anticipated completion date: MCCCD is committed to performing the district-wide IT oversight management process on an annual basis. We respectfully submit that the new oversight management process will address the interests of the Office of the Auditor General as it relates to this finding for the audit period for fiscal year 2018 and on a go-forward basis.

The District agrees to the finding as to the audit period for fiscal year 2017. After the close of the audit period for fiscal year 2017, MCCCD addressed this audit finding by developing an information technology oversight management process to monitor district-wide implementation and application of IT policies and internal controls. The oversight management process was designed and implemented in the first quarter of 2018 and includes the following tools and activities: (1) building of an online application to inventory district-wide adherence to existing Administrative Regulations, IT Directives, and prior IT Audit Findings with associated evidence; (2) evidence of internal control practices provided to District IT Security; (3) reporting results of inventory to CIO; and (4) CIO communication with college and district executive leadership for accountability purposes.

2017-04

The District should improve its risk-assessment process to include information technology security
Names of contact persons: Edward Kelty
Anticipated completion date: **The District anticipates improving its IT risk assessment process in the coming year by improving its process of inventorying, protecting sensitive information, and regularly performing a business impact analysis.**

The District agrees. The District continues to enhance and improve its District-wide Risk Management program as it pertains to IT Risk Management. The District has completed two consecutive District-wide annual IT Risk Assessments as part of the application for Cyber Liability Insurance. As a result of these assessments and demonstrated improvements, cyber insurance coverage has increased from 10,000,000 to 30,000,000 over the past two years.

The District will improve its IT risk assessment process, to ensure that it effectively communicates the results of risk assessments to administration and better document how it prioritizes remediation and responses to the risks it identifies.

2017-05

The District should improve security over its information technology resources
Names of contact persons: Edward Kelty
Anticipated completion date: **The District will update, approve and monitor its information technology and information security policies continuously according to its Internal Control Development process to adapt to the ever-changing control and risk landscape.**

The District agrees. The District has adopted an Administrative Regulation that provides the Vice Chancellor for ITS with the authority to "issue Governance Directives as needed to regulate [the] use of IT resources." Known as Information Technology Directives, these foundational documents shape information security and privacy practices for MCCCD.

Over the past three years, the district has made significant advancements in its control environment by creating and maintaining information security and privacy focused Administrative Regulations and Information Technology Directives. Specifically, MCCCD has developed a process for the drafting and implementation of new control practices (Internal Control Development) calling for (1) the identification of areas for new or updated Administrative Regulations and IT Directives; (2) prioritization of new or updated Administrative Regulations and IT Directives; (3) collection of stakeholder review and comment for draft Administrative Regulations and IT Directives; and (4) executive review and approval.

Beginning 2015, the District continues to add and update Information Technology Directives including:

- Authority and Overview
- Cloud Services
- Compliance
- Employee Termination / Separation
- Governance
- Information Classification and Handling
- Physical Security
- Risk Management
- Technology Use

Information Technology Directives in development include:

- Business Resilience
- Mobile / Bring Your Own Device (BYOD)

2017-06

The District should improve access controls over its information technology resources
Names of contact persons: Edward Kelty
Anticipated completion date: MCCCD is committed to maintaining the access control practices that address the finding for the fiscal year 2017 audit period implemented between 2016 and 2018 and described for finding 2017-06. Further, MCCCD will continue its policy development process in the areas described in 2017-05 and 2017-06 to continuously improve its access controls over its IT resources.

The District agrees to the finding as to the audit period for fiscal year 2017. Notwithstanding its agreement, the District is pleased to report that it has significantly enhanced its policies and procedures to strengthen MCCCD's capabilities in regard to prevention and detection of unauthorized access, manipulation, damage, or loss to it IT resources (see response to 2017-05).

Specifically, in 2016, MCCCD began monitoring and managing privileged access to cloud data with an access control broker. In 2017, a credential management platform was implemented by the District on a limited basis. Shared accounts are now actively managed by this platform. In the first of quarter of 2018, the District adopted two new IT Directives that substantially improve access controls over its IT resources. The first IT Directive adopted and applied the industry-recognized security principle of "Least Required Privileged" to control access and to monitor IT resources. The second notable newly adopted IT Directive was jointly drafted by Human Resources and IT and clearly sets forth criteria for removing access for employees who are no longer employed by Maricopa. Additionally, the District utilizes VPN technology to encrypt and ensure confidentiality of remote access. These strategies will be further supported by an Information Technology Directive in development for a Mobile / Bring Your Own Device (BYOD) directive.

2017-07

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

Names of contact persons: Edward Kelty

Anticipated completion date: The Directive on Business Resilience currently in development is slated to be finalized in 2018.

At this time, practices are in place that provide for the backup and recovery of data. MCCCD contracts for such capabilities with vendors hosting or maintaining data for MCCCD as well. Even so, the District agrees that it should continue improving its contingency planning policies and procedures.

A Directive on Business Resilience that would address contingency planning procedures is in development. A design element for the new policy includes standardization of business resilience practices district-wide. This policy will provide guidance for conducting a business impact analysis, system backups, performing periodic testing, as well as documenting procedures for performing disaster recovery.

ARIZONA
Auditor General
Making a Positive Difference