Maricopa County Community College District

Report on Internal Control and on Compliance

Year Ended June 30, 2018

A Report to the Arizona Legislature

Lindsey A. Perry
Auditor General

ARIZONA Auditor General
Making a Positive Difference

ARIZONA Auditor General

Making a Positive Difference

The Arizona Office of the Auditor General's mission is to provide independent and impartial information and specific recommendations to improve the operations of State and local government entities. To this end, the Office 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 **Rick Gray**, Chair
Senator **Lupe Contreras**
Senator **Andrea Dalessandro**
Senator **David C. Farnsworth**
Senator **David Livingston**
Senator **Karen Fann** (ex officio)

Representative **Anthony T. Kern**, Vice Chair
Representative **John Allen**
Representative **Timothy M. Dunn**
Representative **Mitzi Epstein**
Representative **Jennifer Pawlik**
Representative **Rusty Bowers** (ex officio)

Audit Staff

Donna Miller, Director
Stephanie Gerber, 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

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

ARIZONA AUDITOR GENERAL
LINDSEY A. PERRY

JOSEPH D. MOORE
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, 2018, 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 20, 2018. Our report includes a reference to other auditors who audited the financial statements of the Maricopa County Community College District Foundation (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 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 did identify 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 2018-01 and 2018-04 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 2018-02 and 2018-03 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.

Lindsey Perry, CPA, CFE
Auditor General

December 20, 2018

Financial statement findings

2018-01

Procedures over faculty payroll

Condition and context— During the fiscal year, the District made overpayments and underpayments to faculty in the spring and summer semesters resulting in estimated unresolved net overpayments at fiscal year-end of $232,000 affecting approximately 3,000 faculty employees. This was as a result of the District not ensuring certain changes made to its payroll and student information systems during fiscal year 2018 were functioning properly. These improper payments were only made to certain types of employees which included adjunct faculty who are contracted part-time employees and full-time faculty who earn extra pay for additional teaching assignments. For these types of employees, the District's payroll system captures certain contract and assignment data from the student information system to calculate total payroll amounts. However, as a result of the system changes, the contract assignments in the student information system were not always accurate, causing the payroll system to calculate incorrect payment amounts. Further, the District's changes to its payroll and student information systems included adding a mechanism for electronically reviewing and approving adjunct faculty employment contracts to address our prior-year audit finding over these contracts not always being approved. However, this mechanism was not fully implemented and faculty contracts were not always approved prior to processing payments.

Criteria—The District should have effective internal control policies and procedures to ensure all faculty contract assignments are approved and its IT systems are properly functioning to accurately pay its faculty working at all of its colleges and skill centers.

Effect—In making an estimated $232,000 in net overpayments to faculty employees, the District inappropriately spent public monies and have had to use extra resources to correct the deficiencies and to continue its attempts to collect overpayments.

Cause—The District did not plan appropriately to ensure it thoroughly tested its system changes prior to implementation. Also, the District did not provide adequate training to employees using and entering data into the payroll and student information systems prior to implementing system change.

Recommendation—To help ensure that the District accurately pays its faculty for authorized and valid employment contract and assignment data, the District should ensure its established policies and procedures are accurately updated as needed to address its system changes and include procedures to:

- Monitor the colleges' adherence to its policies and procedures over reviewing and approving faculty employment contracts and assignments and ensuring faculty employees are paid correctly and any overpayments or underpayments are rectified.
- Provide adequate training to employees on its systems, including on any upgrades, to ensure business processes such as processing payroll payments are functioning properly.

In addition, the District should ensure its policies and procedures over future system changes require them to be thoroughly tested and reviewed prior to implementation. This should involve tests with interfacing systems and end users, and a post-implementation review to ensure changes were implemented as designed and approved.

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

The portion of this finding over adjunct faculty contract approvals is similar to prior-year finding 2017-01.

2018-02

Procedures for approving hourly employees' time sheets

Condition and context—The District's policies and procedures require a supervisory review and approval of hourly employees' time sheets within the payroll system either prior to processing payroll or within a reasonable time period after it has processed payroll. To ensure all employees are paid on time, the payroll system allows personnel in the payroll department to process unapproved timesheets for payment. The District paid approximately $31 million to hourly employees during the fiscal year. However, the District had not fully implemented established procedures to ensure that supervisors reviewed and approved hourly employee time sheets either before or after it processed payroll.

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

Effect—The District risks paying for unapproved hours worked, which could potentially result in inappropriate use of public monies. We were unable to determine the total number of time sheets that may not have been approved.

Cause—The District's supervisors did not always follow existing policies and procedures for approving employees' time sheets, and the District did not appropriately follow up to ensure time sheets were reviewed either prior to the employees being paid or within a reasonable time after.

Recommendation—To help ensure that it pays employees only for authorized and approved hours worked, the District should require its existing policies and procedures be followed and monitored for reviewing and approving employees' time sheets. This includes the District's existing policies to review reports within its payroll system to identify and monitor hourly employees' time sheets that were not approved prior to processing their pay and email all supervisors to approve the hourly employees' time sheets or make adjustments accordingly on the next pay cycle.

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 2017-02.

2018-03
Managing risk

Condition and context—The District's process for managing its risks did not include an overall risk-assessment process that included identifying, analyzing, and responding to the District-wide information technology (IT) risks, such as potential harm from unauthorized access, use, disclosure, disruption, modification, or destruction of IT data and systems. Also, it did not include inventorying sensitive information that might need stronger access and security controls and evaluating and determining the business functions and IT systems that would need to be restored quickly if the District were impacted by disasters or other system interruptions.

Criteria—Effectively managing risk at the District includes 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 not only report accurate financial information and protect its IT systems and data but to also carry out its overall mission and service objectives. The process should provide the basis for developing appropriate responses based on identified risk tolerances and specific potential risks to which the District might be subjected. To help ensure the District's objectives can be met, an annual risk assessment should include considering IT risks. For each identified risk, the District should analyze the identified risk and develop a plan to respond within the context of the District's defined objectives and risk tolerances. The process of managing risks should also address the risk of unauthorized access and use, modification, or loss of sensitive information and the risk of losing the continuity of business operations in the event of a disaster or system interruption.

Effect—The District's administration and IT management may put the District's operations and IT systems and data at unintended and unnecessary risk.

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 was still in the process of fully implementing procedures for inventorying, protecting sensitive information, and regularly performing a business impact analysis.

Recommendations—The District should identify, analyze, and reduce risks to help prevent undesirable incidents and outcomes that could impact business functions and IT systems and data. It also should plan for where resources should be allocated and where critical controls should be implemented. To help ensure it has effective entity-wide policies and procedures to achieve these objectives, the District should follow guidance from a credible IT security framework such as that developed by the National Institute of Standards and Technology. Responsible administrative officials and management over finance, IT, and other entity functions should be asked for input in the District's process for managing risk. The District should conduct the following as part of its process for managing risk:

- Perform an annual entity-wide IT risk-assessment process that includes evaluating risks such as risks of inappropriate access that would affect financial data, system changes that could adversely impact or disrupt system operations, and inadequate or outdated system security.
- Evaluate and manage the risks of holding sensitive information by inventorying the information the District holds to assess where stronger access and security controls may be needed to protect data in accordance with state statutes and federal regulations.
- Evaluate and determine the business functions and IT systems that would need to be restored quickly given the potential impact disasters or other IT system interruptions could have on critical organizational

functions such as student services and operations such as payroll and accounting and determine how to prioritize and plan for recovery.

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 2017-04.

2018-04

Information technology (IT) controls—access, security, and contingency planning

Condition and context—The District's control procedures were not sufficiently designed, documented, and implemented to respond to risks associated with its IT systems and data. Further, the District did not clearly designate oversite and monitoring responsibilities to ensure that its business units followed District-wide IT policies and procedures. The District lacked adequate procedures over the following:

- **Restricting access to its IT systems and data—**Procedures did not consistently help prevent or detect unauthorized or inappropriate access.
- **Securing systems and data—**IT security procedures lacked controls to prevent unauthorized or inappropriate access or use, manipulation, damage, or loss.
- **Developing and documenting a contingency plan—**The District should include steps necessary for restoring operations in the event of a disaster or other system interruption.

Criteria—The District should have effective internal controls to protect its IT systems and help ensure the integrity and accuracy of the data it maintains. Further, effective oversight and ongoing monitoring activities are crucial for the District to assess the effectiveness of its IT policies and procedures and take necessary remedial action.

- **Logical and physical access controls—**Help to ensure systems and data are accessed by users who have a need, systems and data access granted is appropriate, key systems and data access is monitored and reviewed, and physical access to system infrastructure is protected.
- **IT security internal control policies and procedures—**Helps prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT systems and data.
- **Comprehensive documented and tested contingency plan—**Provides the preparation necessary to place the plan in operation and helps to ensure business operations continue and systems and data can be recovered in the event of a disaster, system or equipment failure, or other interruption.

Effect—There is an increased risk that the District may not adequately protect its IT systems and data, which could result in unauthorized or inappropriate access and the loss of confidentiality and integrity of systems and data. It also increases the District's risk of not being able to effectively continue daily operations and completely and accurately recover vital IT systems and data in the event of a disaster or system interruption.

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, although the

District centralized some aspects of IT internal controls, it had not clearly designed oversight and monitoring responsibilities of its IT internal controls.

Recommendations—To help ensure the District has effective policies and procedures over its IT systems and data, the District should follow guidance from a credible IT security framework such as that developed by the National Institute of Standards and Technology. Further, the District should clearly designate oversight and perform monitoring activities to ensure its business units follow District-wide IT policies and procedures. To help achieve these control objectives, the District should develop, document, and implement control procedures in each IT control area described below:

Access

- Assign and periodically review employee user access ensuring appropriateness and compatibility with job responsibilities.
- Remove terminated employees' access to IT systems and data.
- Review all other account access to ensure it remains appropriate and necessary.
- Evaluate the use and appropriateness of accounts shared by two or more users and manage the credentials for such accounts.
- Enhance authentication requirements for IT systems.
- Manage employee-owned and entity-owned electronic devices connecting to the District's systems and data.
- Manage remote access to the District's systems and data.
- Review data center physical access periodically to determine whether individuals still need it.

Security

- Perform proactive key user and system activity logging and log monitoring, particularly for users with administrative access privileges.
- Perform IT vulnerability scans and remediate vulnerabilities in accordance with a remediation plan.
- Identify, evaluate, and apply patches in a timely manner.

Contingency planning

- Develop and implement a contingency plan and ensure it includes all required elements to restore critical operations, including being prepared to enable moving critical operations to a separate alternative site if necessary.
- Test the contingency plan.
- Train staff responsible for implementing the contingency plan.
- Back up and securely maintain backups of systems and data.

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 2017-03 (oversight), 2017-06 (access), 2017-05 (IT security), and 2017-07 (contingency planning).

DISTRICT RESPONSE

MARICOPA COMMUNITY COLLEGES

2411 West 14th Street, Tempe, AZ. 85281
T: 480.731.8000 • W: www.maricopa.edu

February 11, 2019

Lindsey Perry
Auditor General
2910 N. 44th St., Ste. 410
Phoenix, AZ 85018

Dear Ms. Perry:

We have prepared the accompanying corrective action plan as required by the standards applicable to financial audits contained in Government Auditing Standards and by the audit requirements of Title 2 U.S. Code of Federal Regulations Part 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards. Specifically, for each finding we are providing you with our responsible officials' views, the names of the contact people responsible for corrective action, the corrective action planned, and the anticipated completion date.

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, 2018

Financial statement findings

2018-01

The District should improve procedures over adjunct faculty payroll

Name(s) of contact person(s): Kim Granio and Martha Anderson

Anticipated completion date: June 2019

The District agrees with the finding. A new requirement to approve assignments is working as designed and is already showing better results for fiscal year 2019.

Regarding the management of the system changes and resulting over and underpayments to faculty, the District has performed faculty pay reconciliations for calendar year 2018 and identified net underpayments and net overpayments to faculty for the calendar year. Most underpayments were $1 or less. Many of the discrepancies were resolved prior to December 31, 2018. The remaining discrepancies were researched in January and any remaining underpayments were processed in January. Overpayments will be resolved prior to March 1, 2019. They take longer because faculty dispute the data which must be reconciled at each college. Throughout the reconciliation process, which entailed significant research by the colleges, the District determined that additional changes were needed to the systems along with significant improvements in the quantity and quality of training provided to end-users as well as changes to information provided to faculty. All such changes were implemented between November 2018 and January 2019, with training and information sessions continuing throughout spring 2019. The District is committed to continually improve its testing of and training for system changes prior to implementation.

2018-02

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

Name(s) of contact person(s): Kim Granio and Barbara Basel

Anticipated completion date: December 2019

The District agrees with the finding. The District's Human Capital Management System (HCM) is not currently configured to require supervisory approvals of time sheets prior to paying employees for hours recorded as Department of Labor regulations require that employees be paid for time worked regardless of approval status. During fiscal year 2016-17, the District developed and implemented a manual approval process for any time worked and paid, but not approved. Unfortunately, with the challenges encountered with the system changes noted in Finding 2018-01, all focus was shifted to resolving pay issues. We will resume efforts prior to the end of Fiscal Year 2018-19 to increase compliance.

Maricopa County Community College District
Corrective Action Plan
Year ended June 30, 2018

2018-03
Managing Risk

Names of contact persons: Mark Koan and Mitchell Kohlbecker

Anticipated completion date: MCCCD expects the full implementation and adoption of NIST standards and related independent risk assessments to be completed by the 4th quarter of calendar year 2021. Execution of an annual internal risk assessment will begin in fiscal year 2019-2020.

The District agrees with the finding. The District is in the process of finalizing its risk mitigation strategy related to entity-wide IT security. The District is in the process of completing a comprehensive IT security risk assessment that will identify any gaps. As part of our initiative to reduce the District IT security threat surface and decrease the risks to information governed by the District, the District has adopted the NIST framework as a set of standards to help inform and enforce information security, risk mitigation, and create a more informed security culture. This set of standards includes an annual entity-wide IT risk assessment conducted by a disinterested third party and a review and continuing implementation of our data classification strategy.

2018-04
Information technology (IT) controls—access, security, and contingency planning

Names of contact persons: Mark Koan and Mitchell Kohlbecker

Anticipated completion date: The District anticipates having all of these initiatives relating to this finding completed by the 2nd quarter of calendar year 2021.

The District agrees with the findings. The District is pleased to report that the findings related to security are remedied or are in the process of remediation. The District has adopted a vulnerability scan process for systems and software that includes a remediation plan for all implementations.

Access

Significant progress is being made in establishing a role-based access controls (RBACs) policy and processes that limit access based on the principle of "least privilege". Establishing effective RBAC policy and processes allows the District to ensure data is accessed only by users that require it and only while they require it. The RBAC policy and processes also improve internal controls, reduce access redundancy, and enhance information security of sensitive and regulated data.

Security

The District recognizes the need for enhanced authentication, improved remote access process/directives, better device management and is developing a comprehensive identity management strategy for the District. We are pleased to note that patch management is being closely monitored. Issues are currently flagged and isolated/remediated as part of our current process to effectively mitigate risks from known vulnerabilities.

Contingency Planning

Maricopa County Community College District
Corrective Action Plan
Year ended June 30, 2018

The District also recognizes the need for contingency planning and has adopted an ITS continuity plan to ensure that in the event of a crisis or data loss, systems remain available and data is recoverable. The execution of the continuity plan directive is underway.


ARIZONA
Auditor General
Making a Positive Difference