Pima 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

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

John Faulk, 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

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

Independent auditors' report on internal control over financial reporting and on compliance and other matters based on an audit of basic financial statements performed in accordance with *Government Auditing Standards*

Members of the Arizona State Legislature

The Governing Board of
Pima County Community College District

We have audited the financial statements of the business-type activities and discretely presented component unit of Pima 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 22, 2017. Our report includes a reference to other auditors who audited the financial statements of the Pima Community College Foundation, Inc., 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 Pima Community College Foundation, Inc., 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 Pima Community College Foundation, Inc.

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.

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. 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.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies, and therefore, material weaknesses or significant deficiencies may exist that have not been identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control, described in the accompanying schedule of findings and questioned costs as items 2017-01 through 2017-06, that we consider 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*.

Pima County Community College District's response to findings

Pima 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 22, 2017

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

Independent auditors' report on compliance for each major federal program; report on internal control over compliance; and report on schedule of expenditures of federal awards required by the Uniform Guidance

Members of the Arizona State Legislature

The Governing Board of
Pima County Community College District

Report on compliance for each major federal program

We have audited Pima County Community College District's compliance with the types of compliance requirements described in the *U.S. Office of Management and Budget (OMB) Compliance Supplement* that could have a direct and material effect on each of its major federal programs for the year ended June 30, 2017. The District's major federal programs are identified in the summary of auditors' results section of the accompanying schedule of findings and questioned costs.

Management's responsibility

Management is responsible for compliance with federal statutes, regulations, and the terms and conditions of its federal awards applicable to its federal programs.

Auditors' responsibility

Our responsibility is to express an opinion on compliance for each of the District's major federal programs based on our audit of the types of compliance requirements referred to above. We conducted our audit of compliance in accordance with U.S. generally accepted auditing standards; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and 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* (Uniform Guidance). Those standards and the Uniform Guidance require that we plan and perform the audit to obtain reasonable assurance about whether noncompliance with the types of compliance requirements referred to above that could have a direct and material effect on a major federal program occurred. An audit includes examining, on a test basis, evidence about the District's compliance with those requirements and performing such other procedures as we considered necessary in the circumstances.

We believe that our audit provides a reasonable basis for our opinion on compliance for each major federal program. However, our audit does not provide a legal determination of the District's compliance.

Opinion on each major federal program

In our opinion, Pima County Community College District complied, in all material respects, with the types of compliance requirements referred to above that could have a direct and material effect on each of its major federal programs for the year ended June 30, 2017.

Other matters

The results of our auditing procedures disclosed instances of noncompliance that are required to be reported in accordance with the Uniform Guidance and that are described in the accompanying schedule of findings and questioned costs as items 2017-101 and 2017-102. Our opinion on each major federal program is not modified with respect to these matters.

Report on internal control over compliance

The District's management is responsible for establishing and maintaining effective internal control over compliance with the types of compliance requirements referred to above. In planning and performing our audit of compliance, we considered the District's internal control over compliance with the types of requirements that could have a direct and material effect on each major federal program to determine the auditing procedures that are appropriate in the circumstances for the purpose of expressing an opinion on compliance for each major federal program and to test and report on internal control over compliance in accordance with the Uniform Guidance, but not for the purpose of expressing an opinion on the effectiveness of internal control over compliance. Accordingly, we do not express an opinion on the effectiveness of the District's internal control over compliance.

Our consideration of internal control over compliance was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control over compliance that might be material weaknesses or significant deficiencies, and therefore, material weaknesses or significant deficiencies may exist that have not been identified. However, as discussed below, we identified certain deficiencies in internal control over compliance that we consider to be a material weakness and a significant deficiency.

A deficiency in internal control over compliance exists when the design or operation of a control over compliance does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, noncompliance with a type of compliance requirement of a federal program on a timely basis. A material weakness in internal control over compliance is a deficiency, or a combination of deficiencies, in internal control over compliance, such that there is a reasonable possibility that material noncompliance with a type of compliance requirement of a federal program will not be prevented, or detected and corrected, on a timely basis. We consider the deficiency in internal control over compliance described in the accompanying schedule of findings and questioned costs as item 2017-101 to be a material weakness.

A significant deficiency in internal control over compliance is a deficiency, or a combination of deficiencies, in internal control over compliance with a type of compliance requirement of a federal program that is less severe than a material weakness in internal control over compliance, yet important enough to merit attention by those charged with governance. We consider the deficiency in internal control over compliance described in the accompanying schedule of findings and questioned costs as item 2017-102 to be a significant deficiency.

The purpose of this report on internal control over compliance is solely to describe the scope of our testing of internal control over compliance and the results of that testing based on the requirements of the Uniform Guidance. Accordingly, this report is not suitable for any other purpose.

Pima County Community College District's response to findings

Pima 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 compliance, and accordingly, we express no opinion on them.

Report on schedule of expenditures of federal awards required by the Uniform Guidance

We have audited the financial statements of the business-type activities and discretely presented component unit of Pima 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. We issued our report thereon dated December 22, 2017, that contained unmodified opinions on those financial statements. Our report also included a reference to our reliance on other auditors. Our audit was conducted for the purpose of forming our opinions on the financial statements that collectively comprise the District's basic financial statements. The accompanying schedule of expenditures of federal awards is presented for purposes of additional analysis as required by the Uniform Guidance and is not a required part of the basic financial statements. Such information is the responsibility of the District's management and was derived from and relates directly to the underlying accounting and other records used to prepare the basic financial statements. The information has been subjected to the auditing procedures applied in the audit of the basic financial statements and certain additional procedures, including comparing and reconciling such information directly to the underlying accounting and other records used to prepare the basic financial statements or to the basic financial statements themselves, and other additional procedures in accordance with U.S. generally accepted auditing standards. In our opinion, the schedule of expenditures of federal awards is fairly stated in all material respects in relation to the basic financial statements as a whole.

Jay Zsorey, CPA
Financial Audit Director

February 15, 2018

Summary of auditors' results

Financial statements

Type of auditors' report issued on whether the financial statements audited were prepared in accordance with generally accepted accounting principles	**Unmodified**
Internal control over financial reporting	
Material weaknesses identified?	**No**
Significant deficiencies identified?	**Yes**
Noncompliance material to the financial statements noted?	**No**

Federal awards

Internal control over major programs	
Material weakness identified?	**Yes**
Significant deficiency identified?	**Yes**
Type of auditors' report issued on compliance for major programs	**Unmodified**
Any audit findings disclosed that are required to be reported in accordance with 2 CFR §200.516(a)?	**Yes**

Identification of major programs

CFDA number	Name of federal program or cluster
84.007, 84.033, 84.063, 84.268	Student Financial Assistance Cluster
84.042, 84.044, 84.047, 84.066	TRIO Cluster
84.031	Higher Education—Institutional Aid

Dollar threshold used to distinguish between Type A and Type B programs	$1,537,950
Auditee qualified as low-risk auditee?	No

Other matters

Auditee's summary schedule of prior audit findings required to be reported in accordance with 2 CFR §200.511(b)?	Yes

Financial statement findings

2017-01

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 risk-assessment process did not include a district-wide information technology (IT) security risk assessment over the District's IT resources, which include its systems, network, infrastructure, and data. Also, the District did not identify and classify sensitive information. 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 has relied on an informal process to perform risk-assessment procedures that did not include IT security.

Recommendations—To help ensure the District has effective policies and procedures to identify, analyze, and respond to risks that may impact its IT resources, the District needs to implement a 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 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.
- **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 updating its disaster recovery plan.

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

2017-02

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 has some written policies and procedures for managing access to its IT resources; however, they lacked critical elements, and the District did not 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 developed some policies and procedures for IT access but did not have a process in place to ensure they were fully implemented, and lacked detailed policies and procedures for some IT access areas.

Recommendations—To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the District needs to review its logical and physical access policies and procedures over its IT resources against current IT standards and best practices, update them where needed, 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, including users with remote access. Also, when an employee's job responsibilities change, a review of their access should be performed to ensure their access is compatible with the new job responsibilities.
- **Improve network and system password policies—**Network and system password policies should be improved and ensure they address all accounts.
- **Manage entity-owned electronic devices connecting to the network—**The use of 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.
- **Review data center access—**A periodic review of physical access granted to the data center should be performed to ensure that it continues to be needed.

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

2017-03

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—The District did not have policies and procedures for managing changes to its IT resources to ensure changes were properly documented, authorized, reviewed, tested, and approved. Also, the District did not have policies and procedures to ensure 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 had not developed sufficient policies and procedures over configuration management.

Recommendations—To help prevent and detect unauthorized, inappropriate, and unintended changes to its IT resources, the District needs to develop configuration management 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.

- **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 systems 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 only essential services are performed and maintain appropriate and secure configuration settings 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.

2017-04

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 fully implement its existing IT security policies and procedures, and in some cases 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 developed some policies and procedures for IT security but did not have a process in place to ensure they were fully implemented, and lacked detailed policies and procedures for some IT security areas.

Recommendations—To help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss of its IT resources, the District needs to review its IT security policies and procedures against current IT standards and best practices, update them where needed, 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.

- **Implement its incident response plan**—The incident response plan should be tested, implemented, and updated as necessary, and staff responsible for the plan should be trained. The plan should coordinate incident-handling activities with contingency-planning activities and incorporate lessons learned from ongoing incident handling in the incident response procedures. Policies and procedures should also follow regulatory and statutory requirements and require making disclosures to affected individuals and appropriate authorities if an incident occurs.
- **Provide training on IT security risks**—A plan should be developed to provide continuous training on IT security risks, including a security awareness training program for all employees that provides a basic understanding of information security, user actions to maintain security, and how to recognize and report potential indicators of security threats, including threats employees generate. Security awareness training should be provided to new employees and on an on-going basis.

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

2017-05

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's contingency plan lacked certain key elements related to restoring operations in the event of a disaster or other system interruption of its IT resources. 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 lacks a sufficiently documented contingency plan and had not developed written policies and procedures over system and data backups.

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 District should review its contingency planning procedures against current IT standards and best practices, update them where needed, and implement them district-wide, as appropriate. 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.

- **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 included at the end of this report.

2017-06

The District should improve its internal control over purchasing

Criteria—An effective purchasing system allows a district to purchase goods and services as economically as possible within acceptable standards of quality. Districts should have internal controls over purchasing that provide adequate authorization of and accountability for district expenses and ensure that procurement policies are consistent with sound business practices.

Condition and context—The District did not always follow its established policies and procedures for purchases and needs to improve some of its policies and procedures over procurement. For example,

- The District did not always complete an approved purchase order prior to receiving goods and services as required under district policy; however, auditors noted that the District obtained authorizing approvals for these purchases prior to payment.
- A purchase was split into two separate transactions to avoid competitive purchasing.

- The District's purchasing procedures did not require an authorizing approval prior to making purchases under blanket purchase orders. In addition, the District did not monitor purchases made under blanket purchase orders to ensure individual and aggregate spending limits were not exceeded.
- District policy requires payment request forms be used solely for purchases less than $1,000; however, some purchases exceeding $1,000 were approved for payment using payment request forms.

Effect—The District may not receive the best possible value for the public monies it spends and did not always comply with its purchasing policies and procedures.

Cause—The District did not have adequate purchasing policies and procedures for all purchases and did not have adequate internal controls in place to ensure compliance with its established purchasing policies and procedures.

Recommendations—To help ensure the District receives the best possible value for the public monies it spends, the District should develop effective purchasing policies and procedures and implement them district-wide. Further, the District should train staff on the policies and procedures and monitor that their purchasing policies and procedures are 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.

Federal award findings and questioned costs

2017-101

Cluster name: **TRIO Cluster**

CFDA numbers and names:
84.042 **TRIO—Student Support Services**
84.044 **TRIO—Talent Search**
84.047 **TRIO—Upward Bound**
84.066 **TRIO—Educational Opportunity Centers**

Award numbers and years: P042A150315-16, P042A151041-16, P042A150997-16, September 1, 2015 through August 31, 2020; P066A160165-16, P044A160351-16, September 1, 2016 through August 31, 2021: P044A110087-15, September 1, 2011 through August 31, 2016; P047A120942-16, P047A120761-16, P047A121407-16, June 1, 2016 through May 31, 2017; P047A120512-16, September 1, 2012 through August 31, 2017; P047A170256-17A, P047A170154-17A, P047A170032-17A, June 1, 2017 through May 31, 2022

Federal agency: **U.S. Department of Education**

Compliance requirement: Eligibility

Questioned costs: None

Criteria—In accordance with 34 Code of Federal Regulations (CFR) §§645.3 and 644.3, participants in Upward Bound (UB) or Educational Opportunity Centers (EOC) programs must be a United States citizen or national or meet one of several other residency requirements. Further, the District is required by 2 CFR §200.303 to maintain effective internal control over its TRIO Cluster to provide reasonable assurance that it is managing the award in compliance with federal statutes, regulations, and the award terms.

Condition and context—The District did not maintain effective internal control to ensure that all TRIO Cluster UB and EOC program participants were eligible. Specifically, for four of five UB participants and eight of eight EOC participants tested, we noted that the District did not obtain or review sufficient documentation to ensure the participant met eligibility requirements as the District relied solely on participant eligibility self-certifications. We performed alternate audit procedures and determined that all four UB participants and two of the eight EOC participants met the eligibility requirements of the program described above. However, our audit procedures were unable to determine whether the remaining six EOC participants were eligible program participants.

Effect—Without sufficient internal controls to determine eligibility, there is an increased risk of program benefits being provided to ineligible participants.

Cause—The District did not have sufficient internal controls in place to ensure that all program participants were eligible.

Recommendation—The District should implement internal control policies and procedures to ensure that an appropriate review of participant eligibility is performed.

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

2017-102

Cluster name: **Student Financial Assistance Cluster**

CFDA numbers and names:
84.007 **Federal Supplemental Educational Opportunity Grants**
84.033 **Federal Work-Study Program**
84.063 **Federal Pell Grant Program**
84.268 **Federal Direct Student Loans**

Award numbers and year: P007A160133, P033A160133, P063P160512 and P268K170512; July 1, 2016 through June 30, 2017

Federal agency: **U.S. Department of Education**

Compliance requirement: Special tests and provisions

Questioned costs: N/A

Criteria—For the Federal Pell Grant and Federal Direct Student Loans programs, 34 Code of Federal Regulations (CFR) §§690.83(b)(2) and 685.309(b) require institutions to notify the National Student Loan Data System (NSLDS) within 30 days of a change in student status or include the change in status in a response to an enrollment reporting roster file within 60 days. Student enrollment status changes include reductions or increases in attendance levels, withdrawals, graduations, or approved leaves-of-absence. In addition, 2 CFR §200.303 requires the District to maintain effective internal control over its Student Financial Assistance Cluster to provide reasonable assurance that the District is managing the award in compliance with federal statutes, regulations, and the award terms.

Condition and context—The District did not have adequate policies and procedures to ensure that all student enrollment status changes were reported to NSLDS within the required time periods. As a result, for 7 of 40 students tested, the District did not report the change within 60 days after an enrollment reporting roster was received from NSLDS.

Effect—The District did not comply with the enrollment reporting requirement of 34 CFR §§685.309(b) and 690.83(b)(2). Consequently, student enrollment statuses in the NSLDS were not always accurate and/or reported in a timely manner. Therefore, if the NSLDS does not accurately reflect students' enrollment on a timely basis, students may not be asked to repay student financial assistance grants and loans if or when required.

Cause—The District used a third-party servicer to report enrollment status changes to NSLDS but did not have adequate internal control procedures to verify that changes were reported to the NSLDS in a timely manner.

Recommendation—The District should develop and implement policies and procedures to ensure that it monitors changes the third-party servicer submits to ensure the student enrollment status changes reported to the NSLDS are reported within required timelines.

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 2016-101.

DISTRICT SECTION

Pima County Community College District
Schedule of expenditures of federal awards
Year Ended June 30, 2017

Federal agency/CFDA number	Federal program name	Cluster title	Pass-through grantor	Pass-through grantor's numbers	Program expenditures	Amount provided to subrecipients
Department of Agriculture						
10 223	Hispanic Serving Institutions Education Grants				$ 32,335	
Department of Interior						
15 224	Cultural and Paleontological Resources Management				5,946	
15 659	National Wildlife Refuge Fund		Arizona Game and Fish Commission	7010 35001 0300048	9,153	
	Total Department of Interior				15,099	
Department of Justice						
16 607	Bulletproof Vest Partnership Program				3,047	
Department of Labor						
17 268	H-1B Job Training Grants		Pima County Community Services	YC-25417-14-60-A-4	25,780	
17 282	Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grants				437,862	$ 48,855
	Total Department of Labor				463,642	48,855
Department of State						
19 040	Public Diplomacy Programs				12,000	
Department of Transportation						
20 616	National Priority Safety Programs		Governor's Office of Highway Safety	2016-405d-008, 2017-405d-026	22,395	
20 701	University Transportation Centers Program		University of Southern California	69A3551747109	12,452	
	Total Department of Transportation				34,847	
National Aeronautics and Space Administration						
43 001	Science		Planetary Science Institute	NNX16AC55A	3,230	
43 008	Education		University of Arizona	NNX15AJ17H	32,811	
	Total National Aeronautics and Space Administration				36,041	
National Endowment for the Humanities						
45 162	Promotion of the Humanities—Teaching and Learning Resources and Curriculum Development				43,277	
National Science Foundation						
47 049	Mathematical and Physical Sciences		University of Arizona	1460828	9,137	
47 050	Geosciences		University of Arizona	1540596	7,770	
47 076	Education and Human Resources		University of Arizona	1625015, 1644899	37,082	
	Total National Science Foundation				53,989	

See accompanying notes to schedule.

Pima County Community College District
Schedule of expenditures of federal awards
Year Ended June 30, 2017

Federal agency/CFDA number	Federal program name	Cluster title	Pass-through grantor	Pass-through grantor's numbers	Program expenditures	Amount provided to subrecipients
Small Business Administration						
59 037	Small Business Development Centers		Maricopa County Community College District	SBHQ-17-B-0026	161,369	
Department of Education						
84 007	Federal Supplemental Educational Opportunity Grants	Student Financial Assistance Cluster			679,173	
84 033	Federal Work-Study Program	Student Financial Assistance Cluster			537,846	
84 063	Federal Pell Grant Program	Student Financial Assistance Cluster			27,087,654	
84 268	Federal Direct Student Loans	Student Financial Assistance Cluster			11,600,923	
	Total Student Financial Assistance Cluster				39,905,596	
84 042	TRIO—Student Support Services	TRIO Cluster			724,900	
84 044	TRIO—Talent Search	TRIO Cluster			392,313	
84 047	TRIO—Upward Bound	TRIO Cluster			986,416	
84 066	TRIO—Educational Opportunity Centers	TRIO Cluster			77,297	
	Total TRIO Cluster				2,180,926	
84 002	Adult Education—Basic Grants to States		Arizona Department of Education	17FAEABE-712501-16B, 17FAEIEL-712501-16B, 17FAEADL-712501-16B, 17FAEAPL-712501-16B, 17FEDWIO-712501-05A	2,126,691	
84 031	Higher Education—Institutional Aid				2,541,946	
84 048	Career and Technical Education—Basic Grants to States		Arizona Department of Education	16FCTDBG-612501-20A, 17FCTDBG-712501-20A	548,012	
	Total Department of Education				47,303,171	
Department of Health and Human Services						
93 093	Affordable Care Act (ACA) Health Profession Opportunity Grants				2,437,688	352,286
93 243	Substance Abuse and Mental Health Services—Projects of Regional and National Significance				274,042	137,682
93 566	Refugee and Entrant Assistance—State/ Replacement Designee Administered Programs		Arizona Department of Economic Security	DES13038227	201,553	
93 859	Biomedical Research and Research Training		University of Arizona	5K12GM000708-17	83,065	
	Total Department of Health and Human Services				2,996,348	489,968
Corporation for National and Community Service						
94 006	AmeriCorps		Arizona Governor's Office of Youth, Faith and Family	AC-VSG-15-090115-13, AC-VSG-15-090115-13Y2	103,512	

See accompanying notes to schedule.

Pima County Community College District
Schedule of expenditures of federal awards
Year Ended June 30, 2017

Federal agency/CFDA number	Federal program name	Cluster title	Pass-through grantor	Pass-through grantor's numbers	Program expenditures	Amount provided to subrecipients
Department of Homeland Security						
97 010	Citizenship Education and Training		Lutheran Social Services of the Southwest	2014-CS-010-000024	6,336	
	Total expenditures of federal awards				$ 51,265,013	$ 538,823

See accompanying notes to schedule.

Pima County Community College District
Notes to schedule of expenditures of federal awards
Year ended June 30, 2017

Note 1 - Basis of presentation

The accompanying schedule of expenditures of federal awards includes the federal grant activity of Pima County Community College District for the year ended June 30, 2017. The information in this schedule is presented in accordance with the requirements of Title 2 U.S. Code of Federal Regulations (CFR) Part 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* (Uniform Guidance).

Note 2 - Summary of significant accounting policies

Expenditures reported on the schedule are reported on the accrual basis of accounting. Such expenditures are recognized following the cost principles contained in the Uniform Guidance, wherein certain types of expenditures are not allowable or are limited as to reimbursement. Therefore, some amounts presented in this schedule may differ from amounts presented in, or used in the preparation of, the financial statements.

Note 3 - Catalog of Federal Domestic Assistance (CFDA) numbers

The program titles and CFDA numbers were obtained from the federal or pass-through grantor or the 2017 *Catalog of Federal Domestic Assistance*.

Note 4 - Indirect cost rate

The District did not elect to use the 10 percent de minimis indirect cost rate as covered in 2 CFR §200.414.

DISTRICT RESPONSE

PimaCountyCommunityCollegeDistrict

District Office

Office of the Executive Vice Chancellor
for Finance and Administration
4905D East Broadway Boulevard
Tucson, Arizona 85709-1200
Telephone (520) 206-4519
Fax (520) 206-4516
www.pima.edu

February 15, 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* 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,

David Bea, Ph.D.
Executive Vice Chancellor for Finance and Administration

Pima County Community College District

Corrective Action Plan

Year Ended June 30, 2017

Financial Statement Findings

2017-01

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

Contact Person: Kurt Myers

Anticipated Completion Date: June 30, 2021

Corrective Action:
PCC Information Technology (IT) is currently reviewing policies and procedures for risk assessment, data classification, and disaster recovery.

Action Steps and Timeframe:

- Consolidate Compliance with Records and Information Office for enhanced coordination and communication of similar activities. By January 30, 2018
- Finalize Data Classification policy and schema. By June 30, 2018
- Develop Disclosure Process for affected parties. By June 30, 2018
- Develop and implement IT risk management plan. By June 30, 2019
- Develop and Implement Business Impact Analysis and Disaster Recovery Plan. By June 30, 2019
- Inventory all data (records) in all mediums and protect sensitive information according to File Plan and Data Classification standards. By June 30, 2021

2017-02

The District should improve access controls over its information technology resources.

Contact Person: Kurt Myers

Anticipated Completion Date: June 30, 2018

Corrective Action:
PCC IT is working with unit stakeholders to develop internal processes and policies to improve logical and physical access over information technology resources. Part of this framework is the updating of our acceptable use agreement which is currently in its final stages before the policy becomes active.

Action Steps and Timeframe:

- Acceptable Use Agreement Final Draft. By March 31, 2018
- Develop standard operating procedure (internal IT policy) for College owned electronic devices. By June 30, 2018
- Formalization of controls for access including; system password, review of user access to systems, data center access and logging/monitoring of administrative accounts protocols. By June 30, 2018

2017-03

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

Contact Person: Kurt Myers

Anticipated Completion Date: June 30, 2019

Corrective Action:
PCC IT is aware that there are limited procedures written for configuration management processes. Currently we have processes for desktop patching and server patching. The Office of Information Assurance and Compliance will work with IT stakeholders to develop a comprehensive policy and procedure handbook to address all systems that IT manages to ensure there are internal control policies to track and document changes made to IT resources.

Action Steps and Timeframe:

- Develop Configuration Management Handbook that addresses process, documents changes and clearly shows the rationale for changes. Include procedures for roll back and testing for each system. By June 30, 2019
- Develop policy and procedure that supports Configuration Management Handbook. By June 30, 2019

2017-04

The District should improve security over its information technology resources.

Contact Person: Kurt Myers

Anticipated Completion Date: December 31, 2018

Corrective Action:
PCC IT is working towards developing a comprehensive cyber security framework that strengthens the incident response plan, incorporates training for internal IT staff and PCC staff. Part of this review is to ensure compliance with NIST 800 framework.

Action Steps and Timeframe:

- Develop Incident Response Plan. Completed
- Develop Mobile Device Management Plan. By August 31, 2018
- Strengthen IT security policies and procedures to ensure they integrate with other IT policies. By December 31, 2018
- Develop training for all PCC Staff regarding cyber security best practices. By December 31, 2018
- Train IT staff and conduct table top exercises for incident response. By December 31, 2018

2017-05

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

Contact Person: Kurt Myers

Anticipated Completion Date: June 30, 2019

Corrective Action:
PCC IT is working towards a comprehensive contingency planning policy and procedure framework. The Office of Information Assurance and Compliance will be working with IT stakeholders to ensure a plan is developed for all systems, testing occurs, training occurs for staff who are responsible for implementation of a contingency plan and that documentation is kept current once developed.

Action Steps and Timeframe:

- Develop policy and procedures to include roles and responsibilities, scope, resource requirements, training, exercise and testing schedules, plan maintenance schedules, minimum frequency of data backups, and documentation of tests performed against policy. By June 30, 2019

2017-06

The District should improve its internal control over purchasing.

Contact Person: Mark Dworschak

Anticipated Completion Date: June 30, 2018

Corrective Action:
The department has developed a Purchasing Administrative Procedure which will be submitted for Board of Governors approval by June 30, 2018. Purchasing procedures are near completion with both department manuals (Purchasing and P-Card) and development of an improved College-wide purchasing system underway. The new system is being developed for purchase requests to connect to approved purchase orders, invoice and payment processing. A payment for an unauthorized purchase will not process without an underlying purchase order. The college is currently in final testing and expects the system roll-out to begin by June 30, 2018.

The revised purchasing procedures will identify, by designated College account codes and accompanying commodity codes, the types of expenses to be processed. Expenditures not subject to the purchasing procedures will be reviewed and processed via payment requests, with the proper approvals. The system will flag improper requests and prevent any attempts to bypass the purchasing process. Training and dissemination of the information about new process and procedures will precede the system's roll-out. Ongoing training to comply with new or changing procedures will be required for all purchasing staff.

Note, even with the system in place, the College anticipates a period (ending by the close of FY 2018) where invoices for *previously* purchased goods and services will still be paid via payment request forms. Because the practice of backdating purchase orders will remain prohibited, the College by default will rely on payment requests as a mechanism to compensate vendors for approved goods and services already delivered. All purchasing policies and procedures, as well as adequate internal controls to ensure adherence to these policies and procedures, will be in place and operational no later than July 1, 2018.

Federal Award Findings

2017-101

CFDA Numbers: 84.042 TRIO—Student Support Services, 84.044 TRIO—Talent Search, 84.047 TRIO—Upward Bound, 84.066 TRIO—Educational Opportunity Centers

Contact Person: Amanda Kaminski

Anticipated Completion Date: June 30, 2018

Corrective Action:

The College has made improvements to ensure verification of program participant eligibility for the TRIO cluster Upward Bound and Educational Opportunity Centers programs. The College has reviewed and updated all TRIO grant procedures, verified with the Federal Program Officers the procedures meet all federal compliance requirements, and implemented in December 2017. The District Grants Resource Office completes annual monitoring visits for Talent Search and Student Support Services and will add Upward Bound in Spring 2018. Each grant Program Manager will complete an internal audit twice a year based on the academic calendar starting in Spring 2018.

The College has made enhancements to the Upward Bound program policies and procedures manuals, which allowed participants to self-declare citizenship. Regulations require maintaining a record of participant's eligibility. The procedure was updated in December 2017 and grant staff is collecting support documentation to verify citizenship for all current participants with an anticipated completion date of February 2018. All four of the students mentioned in the audit met citizenship requirements.

PCC has reviewed the Educational Opportunity Centers grant program policies and procedures, which allowed participants to self-declare citizenship. Regulations require maintaining a record of participant's eligibility. The Educational Opportunity Centers grant ended on 9/30/2017 after one year. The District Grants Office has been able to verify one of the six students met citizenship requirements.

2017-102

CFDA Numbers: 84.007 Federal Supplemental Educational Opportunity Grants, 84.033 Federal Work-Study Program, 84.063 Federal Pell Grant Program, 84.268 Federal Direct Student Loans

Contact Person: Karrie Mitchell

Anticipated Completion Date: June 30, 2018

Corrective Action:

The College has put measures in place, with a full-time staff member dedicated to enrollment reporting and National Student Clearinghouse error resolution. Certain challenges remain related to Clearinghouse processes between the College and NSLDS reporting. First, the Clearinghouse changed the way "errors" are reported to the College for resolution. Essentially each error now has to be resolved twice, resulting in double data-entry and increased turnaround times. Secondly, students who are reported to the Clearinghouse as graduated using NSC Degree Transmission reports at the end of each semester are still being reported to NSLDS as enrolled. This was discovered in early Fall 2017 through discussions with the College's Clearinghouse representatives. They were putting system changes in place to remedy that situation, however, and six of the seven students not reported within 30 days were due to this condition. The College reported the student as graduated, however Clearinghouse processes did not update their status with NSLDS. Also, our students often graduate with

one award but then immediately re-enroll under another program. This new enrollment trumps the graduated indicator with the Clearinghouse, potentially causing this student to be improperly reported to NSLDS. The College is now exiting the student out of the graduated program as an additional step to help with enrollment reporting.

For the seventh student not reported within 30 days, the faculty member had not reported the enrollment change through the Attendance Tracking system during the time allowed. A Memorandum of Expectations was issued to the faculty member and Dean, and additional training has been given to faculty leadership system wide.

The third component being put in place is automation with the College's Student Information System pertaining to non-financial aid recipients who completely withdraw during the semester. This automation will convert their enrollment status to be picked up by the next Clearinghouse extract and properly report to NSLDS. This should be in place during the Spring 2018 semester.

PimaCountyCommunityCollegeDistrict

District Office

Office of the Executive Vice Chancellor
for Finance and Administration
4905D East Broadway Boulevard
Tucson, Arizona 85709-1200
Telephone (520) 206-4519
Fax (520) 206-4516
www.pima.edu

February 15, 2018

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

Dear Ms. Davenport:

We have prepared the accompanying summary schedule of prior audit findings as required 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, we are reporting the status of audit findings included in the prior audit's schedule of findings and questioned costs. This schedule also includes the status of audit findings reported in the prior audit's summary schedule of prior audit findings that were not corrected.

Sincerely,

David Bea, Ph.D.
Executive Vice Chancellor for Finance and Administration

Pima County Community College District
Summary Schedule of Prior Audit Findings
Year Ended June 30, 2017

Status of Federal Award Findings and Questioned Costs

Finding Number: 11-03, 12-102, 2013-101, 2014-101, 2015-101, 2016-101

11-03 CFDA Numbers: 84.007, 84.032, 84.033, 84.038, 84.063, 84.375
12-102 CFDA Numbers: 84.007, 84.033, 84.038, 84.063, 84.268
2013-101 CFDA Numbers: 84.007, 84.033, 84.038, 84.063, 84.268
2014-101 CFDA Numbers: 84.038, 84.063, 84.268
2015-101 CFDA Numbers: 84.063, 84.268
2016-101 CFDA Numbers: 84.007, 84.033, 84.063, 84.268

Program: Student Financial Assistance Cluster

Status: Partially Corrected

Corrective Action:
The College has put measures in place, with a full-time staff member dedicated to enrollment reporting and National Student Clearinghouse error resolution. Certain challenges remain related to Clearinghouse processes between the College and NSLDS reporting.

First, Clearinghouse changed the way "errors" are reported to the College for resolution. Essentially each error now has to be resolved twice, resulting in double data-entry and increased turnaround times.

Secondly, students who are reported to the Clearinghouse as graduated using NSC Degree Transmission reports at the end of each semester are still reported to NSLDS as enrolled. This was discovered in early Fall 2017 through discussions with the College's Clearinghouse representatives. They were putting system changes in place to remedy that situation, however; and six of the seven students not reported within 30 days were due to this condition. The College reported the student as graduated, however Clearinghouse processes did not update their status with NSLDS. Also, our students often graduate with one award but then immediately re-enroll under another program. This new enrollment trumps the graduated indicator with the Clearinghouse, potentially causing this student to be improperly reported to NSLDS. We are exploring potential options for correcting these scenarios.

The third component being put in place is automation with the College's Student Information System pertaining to non-financial aid recipients who completely withdraw during the semester. This automation will convert their enrollment status to be picked up by the next Clearinghouse extract and properly reported to NSLDS. This should be in place during the Spring 2018 semester.

Finding Number: 2016-102

2016-102 CFDA Numbers: 84.007, 84.033, 84.063, 84.268

Program: Student Financial Assistance Cluster

Status: Fully Corrected


ARIZONA
Auditor General
Making a Positive Difference