Coconino County Community College District

Single Audit Report

Year Ended June 30, 2017

A Report to the Arizona Legislature

Debra K. Davenport
Auditor General

ARIZONA Auditor General
Making a Positive Difference

ARIZONA Auditor General

Making a Positive Difference

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

The Joint Legislative Audit Committee

Senator **Bob Worsley**, Chair

Senator **Sean Bowie**

Senator **Judy Burges**

Senator **Lupe Contreras**

Senator **John Kavanagh**

Senator **Steve Yarbrough** (ex officio)

Representative **Anthony Kern**, Vice Chair

Representative **John Allen**

Representative **Rusty Bowers**

Representative **Rebecca Rios**

Representative **Athena Salman**

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

Audit Staff

Jay Zsorey, Director

David Glennon, 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
Coconino County Community College District

We have audited the financial statements of the business-type activities and discretely presented component unit of Coconino 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 1, 2017. Our report includes a reference to other auditors who audited the financial statements of the Coconino Community College 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 Coconino Community College 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 Coconino Community College 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.

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 2017-04, 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*.

Coconino County Community College District's response to findings

Coconino 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 1, 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
Coconino County Community College District

Report on compliance for each major federal program

We have audited Coconino 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, Coconino 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.

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.

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. 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.

Our consideration of internal control over compliance was for the limited purpose described in the first paragraph of this section 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, we identified a deficiency in internal control over compliance, as described in the accompanying schedule of findings and questioned costs as item 2017-101, that we consider to be a material weakness.

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.

Coconino County Community College District's response to findings

Coconino County Community College District's response to the finding identified in our audit is presented in its corrective action plan at the end of this report. The District's response was not subjected to the auditing procedures applied in the audit of compliance, and accordingly, we express no opinion on it.

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 Coconino 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 1, 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

December 1, 2017

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 weaknesses identified?	**Yes**
Significant deficiencies identified?	**None reported**
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
84.002	Adult Education—Basic Grants to States

Dollar threshold used to distinguish between Type A and Type B programs	$750,000
Auditee qualified as low-risk auditee?	Yes

Other matters

Auditee's Summary Schedule of Prior Audit Findings required to be reported in accordance with 2 CFR §200.511(b)?	No

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 information technology (IT) management to determine the risks the District faces as it seeks to achieve its objectives to report accurate financial information and protect sensitive data. An effective risk-assessment process provides the basis for developing appropriate risk responses and should include defining objectives to better identify risks and define risk tolerances, and identifying, analyzing, and responding to identified risks.

Condition and context—The District's annual risk-assessment process did not include a district-wide IT security risk assessment over the District's IT resources, which include its systems, network, infrastructure, and data. Also, the District did not adequately identify and classify sensitive information.

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 relied on an informal process to perform risk-assessment procedures.

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.

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

Condition and context—The District has written policies and procedures for managing access to its IT resources; however, they lacked critical elements.

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 had not reviewed its policies and procedures to ensure they were in line with current IT standards and best practices.

Recommendations—To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the District needs to review its logical 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.
- **Remove terminated employees' access to its IT resources—**Employees' network access should immediately be removed upon their terminations.
- **Review contractor and other nonentity account access—**A periodic review should be performed on contractor and other nonentity accounts with access to an entity's IT resources to help ensure their access remains necessary and appropriate.
- **Review all shared accounts—**Shared network access accounts should be reviewed and eliminated or minimized when possible.
- **Manage shared accounts—**Shared accounts should be used only when appropriate and in accordance with an established policy authorizing the use of shared accounts. In addition, account credentials should be reissued on shared accounts when a group member leaves.
- **Review and monitor key activity of users—**Key activities of users and those with elevated access should be reviewed for propriety.
- **Improve network and system password policies—**Network and system password policies should be improved and ensure they address all accounts.

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 relied on an informal process for managing changes to its IT resources.

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 system(s) impacted, the individual responsible for making the change, test procedures performed and the test results, security impact analysis results, change approvals at each appropriate phase of the change management process, and a post-change review.
- **Roll back changes—**Roll back 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, and maintain configuration settings**—Configure IT resources appropriately and securely, which includes limiting the functionality to ensure only essential services are performed, and maintain configuration settings for all systems.

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 because they reduce the risks that arise from the loss of confidentiality, integrity, or availability of information that could adversely impact the District's operations or assets. Therefore, the District should implement internal control policies and procedures for an effective IT security process that includes practices to help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources.

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

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

Cause—The District relied on an informal process for maintaining security over its IT resources.

Recommendations—To help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources, the District needs to further develop its IT security policies and procedures. The District should review these policies and procedures against current IT standards and best practices and implemented 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.
- **Develop a plan to provide continuous 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.

- **Perform IT vulnerability scans**—A formal process should be developed for vulnerability scans that includes performing vulnerability scans of its IT resources on a periodic basis and utilizing tools and techniques to automate parts of the process by using standards for software flaws and improper configuration, formatting procedures to test for the presence of vulnerabilities, measuring the impact of identified vulnerabilities, and approving privileged access while scanning systems containing highly sensitive data. In addition, vulnerability scan reports and results should be analyzed and legitimate vulnerabilities remediated as appropriate, and information obtained from the vulnerability-scanning process should be shared with other departments of the entity to help eliminate similar vulnerabilities.
- **Protect sensitive or restricted data**—Restrict access to media containing data the entity, federal regulation, or state statute identifies as sensitive or restricted. Such media should be appropriately marked indicating the distribution limitations and handling criteria for data included on the media. In addition, media should be physically controlled and secured until it can be destroyed or sanitized using sanitization mechanisms with the strength and integrity consistent with the data's security classification.

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

CFDA number and name: 84.002 **Adult Education—Basic Grants to States**
Award numbers and years: 17FAEABE-712231-16B, 17FAEAEF-712231-16B, 17FAEADL-712231-16B, 17FAEAPL-712231-16B, 17FAEWIO-712231-05A for July 1, 2016–June 30, 2017
Federal agency: **Department of Education**
Pass-through grantor: Arizona Department of Education
Compliance requirement: Matching
Questioned costs: None

Criteria—The District's grant agreement with the pass-through grantor required the District to match 25 percent of total program expenditures with nonfederal monies based on its proposed matching cost plan that it submitted to the grantor. Further, the District is required by 2 CFR §200.303 to maintain effective internal control over its Adult Education–Basic Grants to States federal award that provides 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 matching costs were accurately estimated or supported, and sufficient to meet the program's 25 percent match for the award period. For instance, the District overestimated matching contributions in its proposed matching cost plan because it used an incorrect award amount to calculate the match. Further, the District did not compare estimated amounts in its proposed plan to actual costs to ensure it met its required match. In addition, the District did not document employee time and effort on federal award activities to support salaries and wages used as matching costs.

Effect—There is an increased risk that the District may not meet its matching requirement if it does not maintain effective internal control to ensure that matching costs are accurately estimated or supported, and sufficient to meet the program's 25 percent match for the award period. The District recalculated the program's 25 percent match using actual costs, and auditors performed additional auditing procedures to determine that the District complied with the program's matching requirement.

Cause—The District did not have adequate written policies and procedures in place to prepare its matching cost plan or review and approve costs identified as contributions to the program's matching cost requirement.

Recommendation—To help ensure the District complies with the program's matching requirement, the District should develop and implement written policies and procedures for preparing its matching cost plan and reviewing and approving costs identified as contributions to the program's matching cost requirement. In addition, program staff knowledgeable of the matching requirement should perform a detailed review of the proposed matching cost plan prior to submitting it to the pass-through grantor to ensure matching costs included in the plan are accurately estimated and sufficient to meet the program's 25 percent match for the award period. Further, program staff should follow district policies and procedures requiring them to document employee time and effort on federal award activities to support salaries and wages used as matching costs.

DISTRICT SECTION

Coconino 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 number	Program expenditures
Department of Labor					
17 282	Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grants				$ 30,660
National Science Foundation					
47 076	Education and Human Resources		Science Foundation Arizona	STEM 605-14	21,272
Department of Education					
84 002	Adult Education—Basic Grants to States		Arizona Department of Education	17FAEABE-712231-16B, 17FAEAEF-712231-16B, 17FAEADL-712231-16B, 17FAEAPL-712231-16B, 17FAEW10-712231-05A	252,936
84 007	Federal Supplemental Educational Opportunity Grants	Student Financial Assistance Cluster			153,487
84 033	Federal Work-Study Program	Student Financial Assistance Cluster			93,984
84 063	Federal Pell Grant Program	Student Financial Assistance Cluster			3,140,506
84 268	Federal Direct Student Loans	Student Financial Assistance Cluster			2,458,434
	Total Student Financial Assistance Cluster				5,846,411
84 042	TRIO—Student Support Services	TRIO Cluster			253,629
84 048	Career and Technical Education—Basic Grants to States		Arizona Department of Education	17FCTDBG-712231-20A, 17FCTPSG-712231-43B, 16FCTDBG-612231-20A, 16FCTPSG-612231-43B	260,389
	Total Department of Education				6,613,365
Department of Health and Human Services					
93 859	Biomedical Research and Research Training		Northern Arizona University	1001966-02	26,032
	Total expenditures of federal awards				$ 6,691,329

See accompanying notes to schedule.

Coconino 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 Coconino 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

Coconino Community College

December 1, 2017

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

Dear Ms. Davenport:

We have prepared the accompanying Corrective Action Plan as required by the standards applicable to financial audits contained in *Government Auditing Standards* 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,

Jami Van Ess
Executive Vice President

Coconino 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 Persons: Ron Hurle, Chief Innovation Officer

Anticipated completion date: June 30, 2019

Corrective Action: Concur. 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 will strive to implement a district-wide IT risk-assessment plan.

2017-02

The District should improve access controls over its information technology resources

Contact Persons: Ron Hurle, Chief Innovation Officer

Anticipated completion date: June 30, 2019

Corrective Action: Concur. To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the District will strive to review its logical 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 will strive to train staff on the policies and procedures.

Coconino County Community College District
Corrective action plan
Year ended June 30, 2017

2017-03

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

Contact Persons: Ron Hurle, Chief Innovation Officer

Anticipated completion date: June 30, 2019

Corrective Action: Concur. To help prevent and detect unauthorized, inappropriate, and unintended changes to its IT resources, the District will strive to develop configuration management policies and procedures. The District will endeavor to review these policies and procedures against current IT standards and best practices and implement them district-wide, as appropriate. Further, the District will strive to train staff on the policies and procedures.

2017-04

The District should improve security over its information technology resources

Contact Persons: Ron Hurle, Chief Innovation Officer

Anticipated completion date: June 30, 2019

Corrective Action: Concur. To help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources, the District will strive to further develop its IT security policies and procedures. The District will endeavor to review these policies and procedures against current IT standards and best practices and implement them district-wide, as appropriate. Further, the District will strive to train staff on the policies and procedures.

Coconino County Community College District
Corrective action plan
Year ended June 30, 2017

2017-101

CFDA Number 84.002 Adult Education – Basic Grants to States

Contact Persons: Siri Mullaney, Dean of Finance
Greg Cross, Adult Education Director

Anticipated completion date: June 30, 2019

Corrective Action: The District will develop and implement written policies and procedures for preparing its matching cost plan and reviewing and approving costs identified as contributions to the program's matching cost requirement. Program staff knowledgeable of the matching requirement will perform a detailed review of the proposed matching cost plan prior to submitting it to the pass-through grantor to ensure matching costs included in the plan are accurately estimated and sufficient to meet the match required in the award period. Program staff will follow District policies and procedures requiring them to maintain time and effort documentation for salaries and wages used as matching costs.


ARIZONA
Auditor General
Making a Positive Difference