Cochise County Community College District

Report on Internal Control and on Compliance

Year Ended June 30, 2018

A Report to the Arizona Legislature

Lindsey A. Perry
Auditor General

ARIZONA Auditor General
Making a Positive Difference

ARIZONA Auditor General

Making a Positive Difference

The Arizona Office of the Auditor General's mission is to provide independent and impartial information and specific recommendations to improve the operations of State and local government entities. To this end, the Office provides financial audits and accounting services to the State and political subdivisions, investigates possible misuse of public monies, and conducts performance audits and special reviews of school districts, State agencies, and the programs they administer.

The Joint Legislative Audit Committee

Senator **Rick Gray**, Chair
Senator **Lupe Contreras**
Senator **Andrea Dalessandro**
Senator **David C. Farnsworth**
Senator **David Livingston**
Senator **Karen Fann** (ex officio)

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

Audit Staff

Donna Miller, Director
Victoria Fisher, Manager and Contact Person

Contact Information

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

(602) 553-0333

www.azauditor.gov

TABLE OF CONTENTS

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

ARIZONA AUDITOR GENERAL
LINDSEY A. PERRY

JOSEPH D. MOORE
DEPUTY AUDITOR GENERAL

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

Members of the Arizona State Legislature

The Governing Board of
Cochise County Community College District

We have audited the financial statements of the business-type activities and discretely presented component unit of Cochise County Community College District as of and for the year ended June 30, 2018, and the related notes to the financial statements, which collectively comprise the District's basic financial statements, and have issued our report thereon dated December 27, 2018. Our report includes a reference to other auditors who audited the financial statements of the Cochise 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 Cochise 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 Cochise 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.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies, and therefore, material weaknesses or significant deficiencies may exist that have not been identified. However, as described in the accompanying schedule of findings and recommendations, we identified certain deficiencies in internal control that we consider to be material weaknesses and significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the District's basic financial statements will not be prevented, or detected and corrected, on a timely basis. We consider the deficiency described in the accompanying schedule of findings and recommendations as item 2018-02 to be a material weakness.

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the deficiency described in the accompanying schedule of findings and recommendations as item 2018-01 to be a significant deficiency.

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*.

Cochise County Community College District's response to findings

Cochise 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.

Donna Miller, CPA
Director, Financial Audit Division

December 27, 2018

Financial statement findings

2018-01

Managing risk

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

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

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

Cause—The District's risk-assessment policies and procedures lacked some critical elements. In addition, policies and procedures were not fully implemented as of June 30, 2018.

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

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

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

This finding is similar to prior-year finding 2017-01.

2018-02

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

Condition and context—The District's control procedures were not sufficiently designed, documented, and implemented to respond to risks associated with its information technology systems and data. The District lacked adequate procedures over the following:

- **Restricting access to its IT systems and data—**Procedures did not consistently help prevent or detect unauthorized or inappropriate access.
- **Configuring systems securely and managing system changes—**Procedures did not ensure IT systems were securely configured and all changes were adequately managed.
- **Securing systems and data—**IT security policies and procedures lacked controls to prevent unauthorized or inappropriate access or use, manipulation, damage, or loss.
- **Updating a contingency plan—**Plan lacked key elements related to restoring operations in the event of a disaster or other system interruption.

Criteria—The District should have effective internal controls to protect its IT systems and help ensure the integrity and accuracy of the data it maintains.

- **Logical and physical access controls—**Help to ensure systems and data are accessed by users who have a need, systems and data access granted is appropriate, key systems and data access is monitored and reviewed, and physical access to system infrastructure is protected.
- **Well-defined documented configuration management process—**Ensures the District's IT systems are configured securely and that changes to the systems are identified, documented, evaluated for security implications, tested, and approved prior to implementation. This helps limit the possibility of an adverse impact on the system security or operations. Separation of responsibilities is an important control for system changes; the same person who has authority to make system changes should not put the change into production. If those responsibilities cannot be separated, a post-implementation review should be performed to ensure the change was implemented as designed and approved.

- **IT security internal control policies and procedures**—Help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT systems and data.
- **Comprehensive documented and tested contingency plan**—Provides the preparation necessary to place the plan in operation and helps to ensure business operations continue and systems and data can be recovered in the event of a disaster, system or equipment failure, or other interruption.

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

Cause—Some of the District's policies and procedures lacked critical elements, and other policies and procedures were not fully implemented as of June 30, 2018.

Recommendations—To help ensure the District has effective policies and procedures over its IT systems and data, the District should follow guidance from a credible IT security framework such as that developed by the National Institute of Standards and Technology. To help achieve these control objectives, the District should further develop, document, and implement control procedures in each IT control area described below:

Access

- Assign and periodically review employee user access ensuring appropriateness and compatibility with job responsibilities.
- Remove terminated employees' access to IT systems and data.
- Review all other account access to ensure it remains appropriate and necessary.
- Evaluate the use and appropriateness of accounts shared by 2 or more users and manage the credentials for such accounts.
- Enhance authentication requirements for IT systems.
- Protect IT systems and data with session time-outs after defined period of inactivity.
- Adopt and enforce an official employee acceptable-use agreement that addresses protecting confidential and sensitive information and consequences for sharing access or inappropriately accessing data.
- Manage employee-owned and entity-owned electronic devices connecting to the District's systems and data.
- Manage remote access to the District's systems and data.
- Segregate public and internal wireless networks and secure internal wireless network access.
- Utilize data-sharing agreements when sharing the District's data, limit the access as appropriate, and enforce data-sharing security restrictions.
- Review data center physical access periodically to determine whether individuals still need it.

Configuration and change management

- Establish and follow a documented change management process.
- Review proposed changes for appropriateness, justification, and security impact.
- Document changes, testing procedures and results, change approvals, and post-change review.
- Develop and document a plan to roll back changes in the event of a negative impact to IT systems.
- Test changes prior to implementation.

- Separate responsibilities for the change management process or, if impractical, perform a post-implementation review to ensure the change was implemented as approved.
- Configure IT resources appropriately and securely and maintain configuration settings.

Security

- Perform proactive key user and system activity logging and log monitoring, particularly for users with administrative access privileges.
- Prepare and implement a security-incident-response plan clearly indicating how to handle and report incidents.
- Provide all employees ongoing training on IT security risks and their responsibilities to ensure systems and data are protected.
- Perform IT vulnerability scans and remediate vulnerabilities in accordance with a remediation plan.
- Identify, evaluate, and apply patches in a timely manner.
- Develop, document, and follow a process for awarding IT vendor contracts.

Contingency planning

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

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

This finding is similar to prior-year findings 2017-02 (access), 2017-03 (configuration and change management), 2017-04 (IT security), and 2017-05 (contingency planning).

DISTRICT RESPONSE

COCHISE COLLEGE
901 North Colombo Avenue • Sierra Vista, AZ 85635-2317 • 520-515-0500 • www.cochise.edu

February 5, 2019

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

Dear Ms. Perry:

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

Please let me know if there are further questions. I can be reached at daviswᵃcochise.edu or 520-515-3623.

Sincerely,

Wendy Davis, Ph.D.
Vice President for Administration and Human Resources

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

Financial statement findings

2018-01
Managing Risk
Name of contact person: Scott Clark (CTO)
Anticipated completion date: December 2019
The District agrees with this recommendation and continues to implement and create the required policies and procedures to support an annual risk assessment plan. This assessment plan will aid the District in identifying risks, analyzing those risks, and determining the best course of action in addressing possible risks that could impact the District's information technology resources.

2018-02
Information technology (IT) controls—access, configuration and change management, security, and contingency planning
Name of contact person: Scott Clark (CTO)
Anticipated completion date: December 2019
The District agrees with this recommendation and continues to implement and create the required policies and procedures to implement and support controls for access, configuration and change management, security, and contingency planning. These policies and procedures will be based on IT industry standards and best practices that will address controls for access, configuration and change management, security, and contingency planning for IT systems and resources.


ARIZONA
Auditor General
Making a Positive Difference