Cochise County Community College District

Lindsey A. Perry
Auditor General

ARIZONA Auditor General
Making a Positive Difference

ARIZONA Auditor General

Making a Positive Difference

The Arizona 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 **Mark Finchem**, Chair
Senator **Flavio Bravo**
Senator **Tim Dunn**
Senator **David C. Farnsworth**
Senator **Catherine Miranda**
Senator **Warren Petersen** (ex officio)

Representative **Matt Gress**, Vice Chair
Representative **Michael Carbone**
Representative **Michele Peña**
Representative **Stephanie Stahl-Hamilton**
Representative **Betty Villegas**
Representative **Steve Montenegro** (ex officio)

Audit Staff

Katherine Edwards Decker, Director
Taryn Stangle, Manager

Contact Information

Arizona Auditor General
2910 N. 44th St., Ste. 410
Phoenix, AZ 85018-7271

(602) 553-0333

contact@azauditor.gov

www.azauditor.gov

TABLE OF CONTENTS

LINDSEY A. PERRY
AUDITOR GENERAL

ARIZONA
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
Cochise County Community College District

We have audited, in accordance with U.S. generally accepted auditing standards and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the U.S. Comptroller General, 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, 2024, 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 30, 2024. Our report includes a reference to other auditors who audited the financial statements of the Cochise College Foundation, Inc., the discretely presented component unit, as described in our report on the District's financial statements. The Foundation's financial statements were not audited in accordance with *Government Auditing Standards*, and accordingly, this report does not include reporting on internal control over financial reporting or instances of reportable noncompliance associated with the Foundation.

Report on 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) as a basis for designing 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 were not identified. However, as described in the accompanying schedule of findings and recommendations, we identified certain deficiencies in internal control that we consider to be material weaknesses and significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the District's basic financial statements will not be prevented, or detected and corrected, on a timely basis. We consider the deficiencies described in the accompanying schedule of findings and recommendations as item 2024-01 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 deficiencies described in the accompanying schedule of findings and recommendations as item 2024-02 to be a significant deficiency.

Report on 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 financial statements. 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*.

District response to findings

Government Auditing Standards requires the auditor to perform limited procedures on the District's responses to the findings identified in our audit that are presented in its corrective action plan at the end of this report. The District is responsible for preparing a corrective action plan to address each finding. The District's responses and corrective action plan were not subjected to the other auditing procedures applied in the audit of the basic financial statements, and accordingly, we express no opinion on them.

Purpose of this report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the District's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the District's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Lindsey A. Perry

Lindsey A. Perry, CPA, CFE
Auditor General

December 30, 2024

Financial statement findings

2024-01

The District did not restrict access to 2 investment accounts to only authorized employees, increasing the risk of fraud and misuse of public monies

Condition—The District did not restrict access to only authorized employees during the fiscal year for 2 investment accounts totaling over $41.8 million in public monies, or 69.3 percent of the District's total bank and investment account balances, as of June 30, 2024. Specifically, for 2 of 13 bank and investment accounts tested, the District did not immediately remove terminated employees' access to perform confidential banking actions for investment accounts, as follows:

	Number of investment accounts	Investment account(s) balance as of June 30, 2024	Access to perform confidential banking actions not immediately removed for terminated employees	Length of time inappropriate access was allowed
Former controller termed in October 2020	2	$41.8 million	Authorized to act on behalf of the District to perform actions such as withdrawing and transferring funds from the account.	Over 3.5 years after employment ended
Former director of finance termed in February 2023	1	$7.6 million[1]	Authorized to act on behalf of the District to perform actions such as withdrawing and transferring funds from the account.	Over 1 year after employment ended

After we brought this to the District's attention, they removed the terminated employees' access for 1 of the 2 investment accounts.

Effect—Although we reviewed these accounts and did not identify any inappropriate transactions during fiscal year 2024, the District's allowing inappropriate access to its investment accounts, including terminated employees' ability to perform confidential banking actions, increases the risk of fraud and misuse of public monies.

Cause—The District did not have a formal process to immediately remove terminated employees' investment account access, including completing required forms to update authorized signers for investment accounts with financial institutions, and did not periodically review and recertify access. Consequently, District officials were unaware of these terminated employees' inappropriate access until we notified them.

Criteria—The District's policy requires the District to protect its assets and safeguard public monies by preventing unnecessary risks such as theft or the safety of its invested principal.[2] Restricting investment account access to only authorized employees by immediately requesting, through required forms, the investing financial institution to remove access upon employee termination and periodically reviewing and recertifying access to only authorized employees is an essential part of internal control standards, such as *Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States, and integral to ensuring monies are not fraudulently or mistakenly misused.[3]

Recommendations—The District should:

1. Restrict investment account access to only authorized employees to safeguard public monies, including immediately removing access for the former terminated employees we identified.
2. Develop and implement policies and procedures to:
   a. Periodically review and recertify access to investment accounts, limiting the ability to perform confidential banking actions to only authorized employees.
   b. Immediately complete required forms to request investing financial institutions to remove all access for terminated employees, including the ability to be an authorized signer.
   c. Review financial institutions' access listings immediately after requesting the investment institution to remove access to verify that only authorized users remain.

The District's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials. We are not required to audit and have not audited these responses and planned corrective actions and therefore provide no assurances as to their accuracy.

---

[1] This investment account totaling $7.6 million is the same account included in the 2 investment accounts totaling $41.8 million at June 30, 2024.

[2] Cochise County Community College District. (2019). 206 Asset Protection.

[3] U.S. Government Accountability Office (GAO). (2014). Standards for internal control in the federal government. Retrieved 1/22/2025 from https://www.gao.gov/assets/670/665712.pdf

2024-02

The District's control procedures over IT systems and data were not sufficient, which increases the risk that the District may not adequately protect those systems and data

Condition—The District's control procedures were not sufficiently implemented to respond to risks associated with its information technology (IT) systems and data. The District lacked sufficient procedures over the following:

- **Restricting access—**Procedures did not consistently help prevent or detect unauthorized or inappropriate access to its IT systems and data.
- **Securing systems and data—**IT security policies and procedures lacked controls to prevent unauthorized or inappropriate access or use, manipulation, damage, or loss.

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/or the loss of confidentiality or integrity of systems and data.

Cause—The District's administration and IT management reported it did not prioritize implementing processes for assigning and reviewing account access and monitoring compliance with its policy requiring annual security awareness training for all employees because of limited staffing resources, such as the District's ability to hire and retain qualified IT personnel.

Criteria—Implementing effective internal controls that follow a credible industry source, such as the National Institute of Standards and Technology, help the District to protect its IT systems and ensure the integrity and accuracy of the data it maintains as it seeks to achieve its financial reporting, compliance, and operational objectives.[1] Effective internal controls include the following:

- **Restrict access through logical controls—**Help to ensure systems and data are accessed by users who have a need, systems and data access granted is appropriate, and key systems and data access is monitored and reviewed.
- **Secure systems and data through 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.

Recommendations—The District should:

1. Make it a priority to implement IT policies and procedures over restricting access and securing systems and data and develop a process to ensure the procedures are being consistently followed.
2. Restrict access to its IT systems and data by implementing processes to assign and periodically review employee user access ensuring appropriateness and compatibility with job responsibilities.
3. Secure IT systems and data by implementing processes to provide all employees ongoing training on IT security risks and their responsibilities to ensure systems and data are protected.

This finding is similar to prior-year finding 2023-02 and was initially reported in fiscal year 2017.

The District's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials. We are not required to audit and have not audited these responses and planned corrective actions and therefore provide no assurances as to their accuracy.

---

[1] The U.S. Department of Education (ED) requires the District to comply with the Gramm-Leach-Bliley Act (Pub. L. No. 106-102) in their student financial assistance program participation agreement with ED. The Act's "Safeguards Rule" requires institutions of higher education to safeguard sensitive student data in accordance with 16 Code of Federal Regulations, Parts 313 and 314.

DISTRICT RESPONSE

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

February 7, 2025

Lindsey Perry
Auditor General
2910 N 44th St, Suite 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 these findings, we are providing you with our responsible officials' views, the names of the contact people responsible for corrective action, the corrective action that has been taken or is planned, and the anticipated completion date.

Sincerely,

Wendy Davis

Wendy Davis, Ph.D.
Executive Vice President for Administration

Financial statement findings

2024-01
The District did not restrict access to 2 investment accounts to only authorized employees, increasing the risk and misuse of public monies.

Name of contact person and title: Wendy Davis (VPA/CFO)
Completion date: October 24, 2024
Agency's response: Concur
The District was made aware of this issue and took steps to correct immediately. The two financial institutions were contacted and the paperwork for the employees to be removed from the accounts was submitted on October 24, 2024. At the time of issuance of the financial statement report on December 30, 2024, one institution had not confirmed the removal of the former Director of Finance, but has since verified the employee has been removed.

Cochise College has drafted an internal policy for updating authorized employee access when an employee changes positions or is no longer employed by the District. Additionally, the District will review authorized signers and users annually to ensure only authorized employees have access to investment accounts.

2024-02
The District's control procedures over access to IT systems and data were not sufficient, which increases the risk that the District may not adequately protect those systems and data

Name of contact person and title: Rob Gibbs (CISO)
Anticipated completion date: June 30, 2025
Agency's response: Concur
Cochise College implemented improvements to its annual security awareness training during Fiscal Year 2024 aimed at ensuring all college employees with access to IT systems completed annual security awareness training. The controls implemented in FY2024 were refined throughout the fall of 2025 to account for several gaps identified as the college executed its mandatory security awareness training for FY2025. The discrepancies identified by the FY2024 audit team have been addressed and process improvements incorporated to ensure similar discrepancies do not re-occur.

Cochise College has identified an approach to addressing the user account review and least access assignment criteria in the audit. The college will complete the reporting and periodic reviews necessary to demonstrate a process for ensuring users have appropriate access and access is reviewed for high risk information on a predictable cadence.


ARIZONA
Auditor General
Making a Positive Difference