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 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 **Nancy Barto**, Chair
Senator **Rosanna Gabaldon**
Senator **David Livingston**
Senator **Juan Mendez**
Senator **Kelly Townsend**
Senator **Karen Fann** (ex officio)

Representative **Joanne Osborne**, Vice Chair
Representative **Timothy M. Dunn**
Representative **Steve Kaiser**
Representative **Jennifer Longdon**
Representative **Pamela Powers Hannley**
Representative **Rusty Bowers** (ex officio)

Audit Staff

Donna Miller, Director
John Faulk, Manager

Contact Information

Arizona Office of the 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 Comptroller General of the United States, 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, 2020, 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 18, 2020. 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.

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.

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 recommendations as items 2020-01 and 2020-02, 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 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

The 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 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 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, CPA, CFE
Auditor General

December 18, 2020

Financial statement findings

2020-01

The District's deficiencies in its process for managing and documenting its risks may put its IT systems and data at unintended and unnecessary risk

Condition—The District's process for managing and documenting 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.

Effect—Without correcting these deficiencies, the District's administration and IT management may put the District's IT systems and data at unintended and unnecessary risk.

Cause—The District did not allocate sufficient resources to fully develop, document, and implement an IT risk assessment process.

Criteria—The District should follow a credible industry source such as the National Institute of Standards and Technology to help effectively manage risk at the District. Effectively managing risk includes an entity-wide risk assessment process that involves members of the District's administration and IT management. The risk assessment should 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 consider 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.

Recommendations—The District should:

1. Allocate sufficient resources to fully develop and implement an IT risk assessment process.
2. Perform an annual entity-wide IT risk assessment process that includes evaluating and documenting risks and safeguards. Such risks may include inappropriate access that would affect financial data, system changes that could adversely impact or disrupt system operations, and inadequate or outdated system security.
3. 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.

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 2019-01.

2020-02

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 developed, documented, and implemented to respond to risks associated with its 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.
- **Managing system configurations and changes—**Procedures did not ensure configuration settings were securely maintained and all IT system 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.

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 did not allocate sufficient resources to develop and document comprehensive IT policies and procedures and ensure the procedures were followed.

Criteria—The District should follow a credible industry source such as the National Institute of Standards and Technology to implement effective internal controls that protect its IT systems and help ensure the integrity and accuracy of the data it maintains, as follows:

- **Restricting access through logical access 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.
- **Managing system configurations and changes through well-defined, documented configuration management process—**Ensures the District's IT system configurations are documented 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's security or operation. Separating 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.
- **Securing 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. Allocate sufficient resources to develop and document comprehensive IT policies and procedures and develop a process to ensure the procedures are being consistently followed.

Restricting access—To restrict access to its IT systems and data, develop, document, and implement processes to:

2. Assign and periodically review employee user access ensuring appropriateness and compatibility with job responsibilities.
3. Remove terminated employees' access to IT systems and data.
4. Review all other account access to ensure it remains appropriate and necessary.
5. Enhance authentication requirements for IT systems.

Managing system configurations and changes—To configure IT systems securely and manage system changes, develop, document, and implement processes to:

6. Establish and follow a documented change management process.
7. Review proposed changes for appropriateness, justification, and security impact.
8. Document changes, testing procedures and results, change approvals, and post-change review.
9. Develop and document a plan to roll back changes in the event of a negative impact to IT systems.
10. Test changes prior to implementation.
11. Separate responsibilities for the change management process or, if impractical, perform a post-implementation review to ensure the change was implemented as approved.
12. Maintain configurations for all system services, assets, and infrastructure; manage configuration changes; and monitor the system for unauthorized or unintended configuration changes.

Securing systems and data—To secure IT systems and data, develop, document, and implement processes to:

13. Perform proactive key user and system activity logging and log monitoring, particularly for users with administrative access privileges.
14. Prepare and implement a security incident response plan clearly stating how to report and handle such incidents.

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 2019-02.

DISTRICT RESPONSE

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

December 18, 2020

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*. 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 that has been taken or is planned, and the anticipated completion date if not already complete.

Sincerely,

Wendy Davis, Ph.D.
Vice President for Administration

Financial statement findings

Managing risk - 2020-01

Allocate resources and perform annual IT Risk Assessment (Recommendations 1 and 2)
David Luna (CIO), Rob Gibbs (CISO) and Ramu Muthiah (Director Information Security and Compliance)
Cochise College views annual IT Risk Assessments as a vital piece of the college's information security program. Cochise College has already implemented corrective actions in this area for this current fiscal year and will continue to evolve and improve on these actions.
Status: Partially complete **- Anticipated completion date**: March 12, 2021

Identify, classify, and inventory sensitive information stored/processed (Recommendation 3)
David Luna (CIO) and Rob Gibbs (CISO)
Cochise College views the identification, classification and inventory of sensitive information as a vital piece of the college's information security program. Cochise College has begun to identify and maintain an inventory of systems that house sensitive data and designing/documenting/implementing sensitive data protection controls.
Status: Partially complete **- Anticipated completion date**: April 30, 2021

Restricted access - 2020-02

Develop and document comprehensive IT policies and procedures (Recommendation 1)
David Luna (CIO) and Rob Gibbs (CISO)
Cochise College has developed and implemented several IT policies and procedures and continues to enhance policies and procedures in accordance with improvements we are making to our security program.
Status: Partially complete – **Anticipated completion date:** April 30, 2021

Review employee access (Recommendations 2 through 4)
David Luna (CIO) and Ramu Muthiah (Director Information Security and Compliance)
Cochise College views the review of employee access to data systems as a vital piece of the colleges information security program. Cochise College has conducted these reviews previously but we now have begun a more standardized and documented process for this review.
Status: Partially complete **- Anticipated completion date**: March 15, 2021

Enhance authentication requirements (Recommendation 5)
David Luna (CIO), Rob Gibbs (CISO) and Ramu Muthiah (Director Information Security and Compliance)
Cochise College agrees that authentication requirements should be enhanced. Cochise College has begun a comprehensive review of authentication requirements and adherence to those requirements
Status: Partially complete **- Anticipated completion date**: April 16, 2021

Managing system configurations and changes - 2020-02

Configuration and management (Recommendations 6-11)
Rob Gibbs (CISO) and Ramu Muthiah (Director Information Security and Compliance)
Cochise College views the configuration and management for changes to systems as a vital piece of the colleges information security program. Cochise College has implemented corrective actions to address these items during the current fiscal year and will continue to evolve and improve on these actions.
Status: Complete

Baseline Configuration (Recommendation 12)
David Luna (CIO) and Rob Gibbs (CISO)

Cochise College views the use and review of baseline configurations as a vital piece of the college's information security program. Cochise College has begun Identifying and prioritizing systems for creation of baseline configurations.
Status: Complete

Securing systems and data - 2020-02

Proactive key user and system activity logging (Recommendation 13)
Rob Gibbs (CISO) and Ramu Muthiah (Director Information Security and Compliance)
Cochise College views the key user and system activity logging and monitoring as a vital piece of the colleges information security program. Cochise College has begun corrective actions for these items and plans to expand these capabilities further during the current fiscal year.
Status: Partially complete **- Anticipated completion date**: April 30, 2021

Prepare and implement Incident Response (IR) Plan (Recommendation 14)
Rob Gibbs (CISO) and Ramu Muthiah (Director Information Security and Compliance)
Cochise College has reviewed, updated and implemented the college's IR plan. To date, Cochise College has completed reviews and training of the IR plan with IR Team.
Status: Complete


ARIZONA
Auditor General
Making a Positive Difference