



# Report on Internal Control and on Compliance Year Ended June 30, 2025

## Maricopa County Community College District

---



**Lindsey A. Perry**  
Auditor General

# Arizona Auditor General's mission

---

The Arizona Auditor General's mission is to provide independent and impartial information, impactful recommendations, and stakeholder education to improve Arizona government for its citizens. To this end, the Office conducts financial statement audits and provides certain accounting services to the State and political subdivisions, investigates possible criminal violations involving public officials and public monies, and conducts performance audits and special reviews of school districts, State agencies, and the programs they administer.

## The Joint Legislative Audit Committee

The Joint Legislative Audit Committee consists of 5 Senate members appointed by the Senate President and 5 House members appointed by the House Speaker. The Committee is responsible for overseeing the Office, including (1) overseeing all audit functions of the Legislature and State agencies, including sunset, performance, special, and financial audits; special research requests; and the preparation and introduction of legislation resulting from audit report findings; (2) requiring State agencies to comply with audit findings and recommendations; (3) receiving status reports regarding the progress of school districts to implement recommendations; and (4) scheduling hearings to review the status of State agencies and school districts.

Senator **Mark Finchem**, Co-chairman

Senator **Flavio Bravo**

Senator **Tim Dunn**

Senator **David C. Farnsworth**

Senator **Catherine Miranda**

Senator **Warren Petersen** (ex officio)

Representative **Matt Gress**, Chairman

Representative **Michael Carbone**

Representative **Michele Peña**

Representative **Stephanie Stahl-Hamilton**

Representative **Betty Villegas**

Representative **Steve Montenegro** (ex officio)

## Audit staff

**Katherine Edwards Decker**, Director

**Vicki Fisher**, Manager

## Contact information

 (602) 553-0333

 [contact@azauditor.gov](mailto:contact@azauditor.gov)

 [www.azauditor.gov](http://www.azauditor.gov)

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

# TABLE OF CONTENTS

<b>INDEPENDENT AUDITORS' REPORT</b> on internal control over financial reporting and on compliance and other matters based on an audit of basic financial statements performed in accordance with <i>Government Auditing Standards</i>	1
--	---

<b>SCHEDULE OF FINDINGS AND RECOMMENDATIONS</b>	3
---	---

<b>FINANCIAL STATEMENT FINDING: 2025-01</b>	4
---	---

District supervisors not reviewing and approving 2,433 employee time sheets representing \$2.87 million in total wages and District not retaining documentation supporting \$1,009 in payroll costs increased the risk of fraud and potential misuse of public monies

<b>FINANCIAL STATEMENT FINDING: 2025-02</b>	7
---	---

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

<b>FINANCIAL STATEMENT FINDING: 2025-03</b>	9
---	---

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

## **DISTRICT RESPONSE AND CORRECTIVE ACTION PLAN**

### **REPORT ISSUED SEPARATELY**

Annual Comprehensive Financial Report



**ARIZONA  
AUDITOR  
GENERAL**

Lindsey A. Perry, 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  
Maricopa 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 Maricopa County Community College District as of and for the year ended June 30, 2025, 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 19, 2025. Our report includes a reference to other auditors who audited the financial statements of the Maricopa County Community College Foundation, the discretely presented component unit, as described in our report on the District's financial statements.

**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.

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 were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We identified certain deficiencies in internal control, described in the accompanying schedule of findings and recommendations as items 2025-01, 2025-02, and 2025-03, that we consider to be significant deficiencies.

## **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 19, 2025

# SCHEDULE OF FINDINGS AND RECOMMENDATIONS

The subsequent pages present the Arizona Auditor General’s findings and recommendations resulting from our audit of the District’s financial statements.

---

## **District supervisors not reviewing and approving 2,433 employee time sheets representing \$2.87 million in total wages and District not retaining documentation supporting \$1,009 in payroll costs increased the risk of fraud and potential misuse of public monies**

---

### **Condition**

The District reported to us that during fiscal year 2025, and contrary to its written procedures, supervisors had not reviewed or approved—either before processing payroll or within a reasonable amount of time thereafter—2,433 employee time sheets totaling approximately \$2.87 million in total wages. Further, contrary to State law and District policies, the District did not retain documentation supporting \$1,009 in payroll costs. Specifically, for 4 of 40 payroll transactions we tested, the District did not retain documentation to support employees’ pay rates and position assignments, such as approved offer letters, contracts, and personnel action forms, totaling \$1,009.

### **Effect**

The District’s failure to approve time sheets and retain documentation supporting payroll costs increased the risk of fraud and misuse of public monies because it could not prevent, or detect and correct, employees intentionally or unintentionally misreporting their time worked or leave taken, and may have inappropriately paid employees for unapproved work assignments or with inaccurate pay rates.

### **Cause**

Some supervisors did not follow District policies and procedures requiring employees’ time sheets to be reviewed and approved either before processing payroll or within 3 business days from receiving a payroll email notification that the employee’s time sheet needs approval. The District did not provide training for these supervisors to ensure they were aware of the policies and procedures and how to perform and ensure compliance with them.

Additionally, District management did not sufficiently monitor whether each college’s Human Resources Department enforced policies and procedures or verified that supervisors reviewed and approved employees’ time sheets, as required.

Further, the District’s policies and procedures lacked requirements to document all employment offers, including temporary employment offers or changes in position, and retain approved documentation supporting positions and pay rates for all employees.

## Criteria

The District's written procedures require each employee's time sheet to be reviewed and approved by the employee's supervisor either before processing payroll or within 3 business days from receiving a payroll email notification that the employee's time sheet needs approval. Additionally, each college's Human Resources Department is responsible for verifying that supervisors timely reviewed and approved time sheets.<sup>1</sup> Further, State law and the District's record retention policies require the District to retain all public records, including those contained in personnel files, for a period of 5 years after an employee's termination (A.R.S. §39-101).<sup>2,3</sup> Finally, designing, implementing, and maintaining effective policies and procedures over payroll functions are necessary to achieve the District's objectives that include safeguarding public monies and other assets, and responding to risks of fraud is an essential part of internal control standards, such as the *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.<sup>4</sup>

## Recommendations to the District

1. Enforce District written procedures and train responsible supervisors to review and approve employees' time sheets, either before payroll is processed or within 3 business days from receiving the payroll email notification that a time sheet needs approval, to verify employees accurately reported their time worked and leave taken.
2. Update the District's policies and procedures requirements and train responsible employees to ensure departments retain documentation supporting employees' pay rates and position assignments, including approved offer letters, contracts, and personnel action forms for all types of employment offers, including those for temporary employment and changes in position.

Monitor and ensure each college's Human Resources Department:

3. Verifies that supervisors perform the required post-payroll reviews and approvals within 3 business days if situations occur that result in supervisors being unable to conduct time sheet approvals prior to payroll-processing deadlines.
4. Corrects any errors noted during the post-payroll reviews.

This finding is similar to prior-year finding 2024-01 and was initially reported in fiscal year 2014.

---

<sup>1</sup> Maricopa County Community College District. Version 1.1 (2019). Monitoring Time Approvals: Monitoring Procedures.

<sup>2</sup> Maricopa County Community College District. (2025). Staff Policy Manual (Policy B-10: Personnel Files).

<sup>3</sup> Arizona State Library, Archives and Public Records. (2025) General Retention Schedule Created for All Public Bodies (Record Series #20704). Retrieved 11/18/2025 from <https://azlibrary.gov/sites/default/files/docs/General-Retention-Schedule-2025-1015.pdf>

<sup>4</sup> U.S. Government Accountability Office. (2014). *Standards for Internal Control in the Federal Government*. Retrieved 10/14/2025 from <https://www.gao.gov/assets/gao-14-704g.pdf>

## **Views of responsible officials**

The District's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials regarding these recommendations. 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.

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

---

### Condition

The District's process for managing and documenting its risks did not include an overall risk assessment process that included analyzing and responding to the identified District-wide information technology (IT) risks, such as potential harm from unauthorized access, use, disclosure, disruption, modification, or destruction of IT systems and data. Also, its policies and procedures did not include identifying, classifying, and inventorying sensitive information that might need stronger access and security controls.

### Effect

The District's administration and IT management may put the District's operations and IT systems and data at unintended and unnecessary risk of potential harm.

### Cause

The District's administration and IT management reported they have a process to monitor its District office's and colleges' adherence to the District's annual risk assessment policies but did not prioritize completing an analysis and remediation of identified risks by fiscal year-end.<sup>1</sup> Further, the District did not prioritize developing formalized policies and procedures over inventorying its data.

### Criteria

Establishing a process for managing risk that follows a credible industry source, such as the National Institute of Standards and Technology, helps the District to effectively manage risk related to IT systems and data. Effectively managing risk includes an entity-wide risk assessment process that involves members of the District's administration and IT management. An effective risk assessment process helps the District determine the risks it faces as the District 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 compliance and service objectives.<sup>2</sup>

---

<sup>1</sup> The District's policies require a risk assessment to be performed annually (Maricopa County Community College District. [June 30, 2016]. Information Technology Directives Risk Management).

<sup>2</sup> 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.

Additionally, an effective risk management process provides the District the basis for developing appropriate responses based on identified risk tolerances and specific potential risks to which it might be subjected. To help ensure the District's objectives can be met, an effective annual risk assessment considers and identifies IT risk in the District's operating environment, analyzes and prioritizes each identified risk, and develops a plan to respond to each risk within the context of the District's defined objectives and risk tolerances. Finally, effectively managing risk includes the District's process for identifying, classifying, and inventorying sensitive information that might need stronger access and security controls to address the risk of unauthorized access and use, modification, or loss of that sensitive information.

## **Recommendations to the District**

- 1.** Make it a priority to implement processes to monitor its District office's and colleges' adherence to the District's annual risk assessment policies and manage risks and data to determine where to implement critical controls.
- 2.** Make it a priority to develop and implement policies and procedures for a data inventory process.
- 3.** 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.
- 4.** 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.

This finding is similar to prior-year finding 2024-02 and was initially reported in fiscal year 2024.

## **Views of responsible officials**

The District's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials regarding these recommendations. 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.

## 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 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 did not make it a priority to develop and document comprehensive IT policies and procedures and develop a process to ensure the procedures are being consistently followed.

### 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.<sup>1</sup>

---

<sup>1</sup> 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.

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 are 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 to the District

1. Make it a priority to develop and document comprehensive IT policies and procedures and develop a process to ensure the procedures are being consistently followed.
2. Monitor District employees' adherence to the IT policies and procedures on a periodic basis to ensure they are consistently followed and inform employees of updates to the policies and procedures throughout the year.

### Restrict access

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

3. Assign and periodically review employee user access ensuring appropriateness and compatibility with job responsibilities.
4. Remove terminated employees' access to IT systems and data.
5. Review all other account access to ensure it remains appropriate and necessary.
6. Evaluate the use and appropriateness of accounts shared by 2 or more users and manage the credentials for such accounts.
7. Enhance authentication requirements for IT systems.

### Secure systems and data

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

8. 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 2024-03 and was initially reported in fiscal year 2023.

## **Views of responsible officials**

The District's corrective action plan at the end of this report includes the views and planned corrective action of its responsible officials regarding these recommendations. 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.

**The subsequent pages were written by the District to provide a response to the findings and to indicate its intention regarding implementation of the recommendations resulting from the audit conducted by the Arizona Auditor General.**

---



---

2411 W. 14th Street, Tempe, Arizona 85281 - 6942 • T 480.731.8000 • F 480.731.8506 • [www.maricopa.edu](http://www.maricopa.edu)

February 10, 2026

Lindsey A. 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 people responsible for corrective action, the corrective action planned, and the anticipated completion date.

Sincerely,

A handwritten signature in black ink that reads 'Kimberly Brainard Granio'.

Kimberly Brainard Granio, CPA, M.ED.  
Vice Chancellor, Business Services

# Maricopa County Community College District

## Corrective Action Plan

Year ended June 30, 2025

### Financial statement findings

2025-01

**District supervisors not reviewing and approving 2,433 employee time sheets representing \$2.87 million in total wages and District not retaining documentation supporting \$1,009 in payroll costs increased the risk of fraud and potential misuse of public monies.**

*Names of contact person: Kristina Winterstein and Mum Martens*

Anticipated completion date: June 30, 2026

The District agrees with the finding. The District's Human Capital Management System (HCM) is configured to require supervisory approval of employee time sheets. However, Department of Labor regulations require employees to be paid for all time worked regardless of approval status, which may result in payroll processing prior to supervisory approval. To mitigate this risk, as of January 2025, the District has implemented new system controls, new supervisor notifications, additional post-payroll verification procedures and additional monitoring from Human Resources (HR) to ensure employee time worked is reviewed, approved, and corrected, as necessary.

At the beginning of each pay period, dynamic calendar invitations are sent to individuals who should be approving time for that particular pay period. This invitation acts as a reminder to approve employee time by the designated deadline. In addition to the calendar reminder a dynamic email is also sent to individuals who need to approve time each pay period outlining specific detail for time approval for that pay period. On the day time approval is due, another dynamic email is sent to individuals who have not completed time approval. Emails are sent at multiple times during the day until time is approved. Furthermore, if a change is made to an employee time sheet after supervisory approval which requires reapproval, multiple emails are sent to ensure reapproval by the designated deadline.

District procedures following each pay period to ensure compliance have also been enhanced to provide both District and College leadership with information regarding supervisor non-approval. After each pay period, a list of supervisors that did not approve time is sent to leadership. An email with specific instructions is sent to the supervisor to verify and validate employee time worked. Applicable HR offices are also included in the email notification to ensure completion and to update HCM once approval is received.

The District will update procedures and provide training to ensure retention of offer letters, contracts, and personnel action forms for all employee types, including temporary assignments, in accordance with State law and District retention requirements.

Maricopa County Community College District  
Corrective Action Plan  
Year ended June 30, 2025

2025-02

**The District's deficiencies in its process for managing and documenting its risks may put its operations and IT systems and data at unintended and unnecessary risk of potential harm.**

*Name of contact person: Jamie Spradlin*

Anticipated completion date: June 2026

The District agrees with the finding. An institution-wide Data Governance committee has been established and tasked with developing comprehensive policies and procedures to guide data governance practices.

A comprehensive District-wide risk assessment was completed in FY2025. The scheduling details, along with a letter from the vendor outlining the scope and timeline of this assessment, were provided to the audit team. While certain measures to mitigate identified risks are already in place, the District is implementing additional protocols to further enhance the IT security systems and safeguard sensitive data.

2025-03

**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.**

*Name of contact person: Jamie Spradlin*

Anticipated completion date: June 2026

The District agrees with the finding. Updated directives were published in November 2025. The directives have been updated and will be reviewed annually. These changes will be communicated institution wide.

The District has initiated the implementation of a new Identity and Access Management (IAM) solution to strengthen access controls and governance. This initiative includes enhancements to existing review and recertification processes, with plans to broaden their scope and ensure consistent application access all account types. Additional measures are being developed to improve account lifecycle management, enforce compliance with established standards, and address shared account usage, credential security, and training-related access requirements. These efforts aim to develop a more robust and streamlined framework for managing user access and safeguarding critical systems.