

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

## **Maricopa County**

---



**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

**Michelle Walters**, 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> The County'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	4
<b>FINANCIAL STATEMENT FINDING 2025-02</b> The County's control procedures over IT systems and data were not sufficient, which increases the risk that the County may not adequately protect those systems and data	6

## COUNTY 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 Board of Supervisors of  
Maricopa County, Arizona

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 governmental activities, aggregate discretely presented component units, each major fund, and aggregate remaining fund information of Maricopa County as of and for the year ended June 30, 2025, and the related notes to the financial statements, which collectively comprise the County's basic financial statements, and have issued our report thereon dated December 18, 2025. Our report includes a reference to other auditors who audited the financial statements of the Stadium District, Risk Management, Employee Benefits Trust, Housing Authority, and Industrial Development Authority, as described in our report on the County's financial statements. This report includes our consideration of the results of the other auditors' testing of internal control over financial reporting and compliance and other matters that are reported on separately by those other auditors. However, this report, insofar as it relates to the results of the other auditors, is based solely on the reports of the other auditors.

### **Report on internal control over financial reporting**

In planning and performing our audit of the financial statements, we considered the County'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 County's internal control. Accordingly, we do not express an opinion on the effectiveness of the County'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 County'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 and the other auditors 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 and 2025-02, that we consider to be significant deficiencies.

## **Report on compliance and other matters**

As part of obtaining reasonable assurance about whether the County'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*.

## **County response to findings**

*Government Auditing Standards* requires the auditor to perform limited procedures on the County's responses to the findings identified in our audit that are presented in its corrective action plan at the end of this report. The County is responsible for preparing a corrective action plan to address each finding. The County'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 County'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 County'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 18, 2025

# SCHEDULE OF FINDINGS AND RECOMMENDATIONS

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

---

## **The County'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 County's process for managing and documenting its risks did not include identifying, classifying, and inventorying sensitive information that might need stronger access and security controls.

### **Effect**

The County's administration and Information Technology (IT) management may put the County's operations and IT systems and data at unintended and unnecessary risk of potential harm.

### **Cause**

The County's administration and IT management partially implemented requirements in its new data classification policy that was adopted during fiscal year 2025. However, policy requirements were not fully integrated across all the County's applications and financial systems due to the complexity of the classification effort, the number of systems involved, and the volume of data. Further, its policy lacked requirements to perform an inventory of sensitive information in the County's applications and financial systems.

### **Criteria**

Establishing a process for managing risk that follows a credible industry source, such as the National Institute of Standards and Technology, helps the County to effectively manage risk related to IT systems and data. Effectively managing risk includes the County'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 County**

1. Complete implementation of policies and procedures to effectively manage risk related to IT systems and data.
2. Evaluate and manage the risk of holding sensitive information by identifying, classifying, and inventorying the information the County 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 2024-01 and was initially reported in fiscal year 2017.

## **Views of responsible officials**

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

---

### **Condition**

The County's control procedures were not sufficiently developed, documented, and implemented to respond to risks associated with its Information Technology (IT) systems and data.

The County 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.

#### **► Ensuring operations continue**

Contingency plan lacked key elements related to restoring operations in the event of a disaster or other system interruption.

### **Effect**

There is an increased risk that the County 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. It also increases the County'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

The County's administration and IT management reported that it partially implemented multiple control activities related to access management, change management, and account lifecycle governance during the audit period, but due to control environment sequencing and maturity considerations, established procedures were not fully implemented in the following areas:

### ► **Restricting access**

Implementing a process to ensure its IT policies and procedures for restricting logical access to IT systems and data were consistently followed.

### ► **Managing system configurations and changes**

Implementing recent changes to its policies and procedures to manage configurations and changes.

### ► **Securing systems and data**

Developing policies and procedures to monitor system activity for users with administrative access privileges as resources were focused on the implementation of a new financial system.

### ► **Ensuring operations continue**

Testing its disaster recovery plan for 1 of its financial systems that will be replaced during the next fiscal year.

## Criteria

Implementing effective internal controls that follow a credible industry source, such as the National Institute of Standards and Technology, help the County 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.

Effective internal controls include the following:

### ► **Restrict access through logical controls**

Helps 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.

### ► **Manage system configurations and changes through a well-defined, documented configuration management process**

Ensures the County's IT system configurations changes 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.

► **Secure systems and data through IT security internal control policies and procedures**

Helps prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT systems and data.

► **Ensure operations continue through a 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.

## **Recommendations to the County**

- 1.** Monitor County employees' adherence to the access and contingency-planning IT policies and procedures on a periodic basis to ensure they are consistently followed.
- 2.** Develop, document, and/or implement IT policies and procedures for configuration and change management and logging and monitoring of users with administrative access, and train employees on new procedures.

### **Restrict access**

To restrict access to its IT systems and data, implement processes to ensure access control policies are consistently applied, including the following:

- 3.** Assign, periodically review, and document review of 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.** Enhance authentication requirements for IT systems.

### **Manage system configurations and changes**

To configure IT systems securely and manage system changes, implement processes to:

- 7.** Review proposed changes for security impact.
- 8.** Document a plan to roll back changes in the event of a negative impact to IT systems.

### **Secure systems and data**

To secure IT systems and data, implement processes to:

- 9.** Perform proactive key user and system activity logging and log monitoring, particularly for users with administrative access privileges.

## **Ensure operations continue**

To ensure operations continue, implement processes to:

- 10.** Test the contingency plan.

This finding is similar to prior-year finding 2024-02 and was initially reported in fiscal year 2023.

## **Views of responsible officials**

The County'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.

# COUNTY RESPONSE AND CORRECTIVE ACTION PLAN

**The subsequent pages were written by the County 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.**

---



301 W. Jefferson St., 9<sup>th</sup> Floor  
Phoenix, Arizona 85003

February 5, 2026

P: 602-506-3561  
F: 602-506-4451

**Maricopa.gov**

Lindsey Perry  
Auditor General  
2910 North 44th Street, 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 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 "Michael McGee".

Michael McGee  
Chief Financial Officer

**2025-01** The County'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.

**Contact person(s):** Kevin Westover, Customer Experience Officer, Enterprise Technology and Innovation

**Anticipated Completion Date:** June 30, 2026

**Concur.** Maricopa County takes all IT audit findings seriously and has made significant efforts to address identified deficiencies. Although the County has adopted its established policies and procedures, they were not fully implemented as of June 30, 2025, which resulted in this repeat finding.

**2025-02** The County's control procedures over IT systems and data were not sufficient, which increases the risk that the county may not adequately protect those systems and data.

**Contact person(s):** Kevin Westover, Customer Experience Officer, Enterprise Technology and Innovation; James Moore, Chief Information Officer, Maricopa County Treasurer's Office; Bridget Harper, Deputy Finance Director, Office of Budget and Finance; and Emily Parish, Director, Human Resources

**Anticipated Completion Date:** June 30, 2026

**Concur.** Maricopa County takes all IT audit findings seriously and has made efforts to address identified deficiencies. The County will continue to follow established procedures and strengthen access controls over its IT resources.