Office of the Arizona State Treasurer

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 financial statements performed in accordance with *Government Auditing Standards*

Members of the Arizona State Legislature

The Honorable Kimberly Yee
Office of the Arizona State Treasurer

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 investment pools and individual investment account of the Office of the Arizona State Treasurer (Office) as of and for the year ended June 30, 2024, and the related notes to the financial statements, which collectively comprise the Office's financial statements, and have issued our report thereon dated October 31, 2024.

Report on internal control over financial reporting

In planning and performing our audit of the financial statements, we considered the Office'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 financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Office's internal control. Accordingly, we do not express an opinion on the effectiveness of the Office'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 Office's 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 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 deficiency 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 Office's 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 instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* and that are described in the accompanying schedule of findings and recommendations as item 2024-01.

Office response to findings

Government Auditing Standards requires the auditor to perform limited procedures on the Office's responses to the findings identified in our audit that are presented in its corrective action plan at the end of this report. The Office is responsible for preparing a corrective action plan to address each finding. The Office's responses and corrective action plan were not subjected to the other auditing procedures applied in the audit of the 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 Office'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 Office'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

October 31, 2024

Financial statement findings

2024-01

The Office of the Arizona State Treasurer (Office) did not remove 2 former employees' capabilities related to 8 bank accounts and 1 financial investment portfolio, increasing the risk of fraud and misuse of public monies

Condition—The Office did not remove 2 former employees' capabilities related to 8 bank accounts and 1 financial investment portfolio during the fiscal year. Specifically, for 8 of 12 bank accounts and 1 of its financial investment portfolios, 2 former deputy treasurers still had capabilities to perform certain banking actions, as shown in the table below.

Specifically, a former deputy treasurer was an authorized signer on 1 financial institution portfolio with a total ending balance of $891.3 million as of June 30, 2024, for 3 months after employment ended. The same former deputy treasurer remained a signer on 7 bank accounts with a total ending balance of $293.7 million as of June 30, 2024, for 4 months after employment ended. Finally, a different former deputy treasurer remained a signer on 4 bank accounts with an ending balance of $17.4 million as of June 30, 2024, for 6 years after employment ended.

	Bank account/ investment portfolio	Bank account/ balance as of June 30, 2024	Banking actions capabilities not immediately removed for former deputy treasurers	Length of time inappropriate capabilities were allowed
Former deputy treasurer who left employment in April 2024	1 financial institution within the investment portfolio	$891.3 million	Authorized signer with additional privileges, including the ability to order the transfer or delivery of any securities or funds	Over 3 months after retirement
	7 bank accounts	$293.7 million	Ability to perform transfers between State of Arizona bank accounts	Over 4 months after retirement
Former deputy treasurer who left employment in March 2018	4 bank accounts[1]	$17.4 million	Ability to perform transfers between State of Arizona bank accounts	Over 6 years after employment ended

Finally, the Office communicated verbally with the financial institution that held its investment portfolio of $31.2 billion as of June 30, 2024, to remove a former deputy treasurer as the legal designee. Although the

financial institution had controls in place to verify changes to account signers, this former deputy treasurer who left employment in April 2024 remained the legal designee until the Office provided written legal documentation to update the designee with the financial institution over 3 months after this former employee's departure.

Effect—Although we reviewed these accounts and did not identify any inappropriate transactions during fiscal year 2024, the Office's not removing former employees' capabilities related to its bank and investment accounts increased the risk of fraud and misuse of public monies.

Cause—The Office did not have a formal process to immediately notify the financial institutions in writing of changes to former employees' capabilities related to bank and financial investment accounts and update documentation to remove former employees from bank and investment accounts or periodically review and recertify capabilities. The Office reported that it had an informal process to communicate changes to capabilities to the investing financial institutions. However, it did not verify that the change occurred based on this informal communication, and therefore, Office officials were not aware of these former employees' inappropriate capabilities related to the accounts until we notified them.

Criteria—State law requires the Office to safeguard public monies (Arizona Revised Statutes §35-317). Restricting capabilities related to bank accounts and investment portfolios to only authorized employees by immediately requesting, through formal written communication or required forms, the banking or investing financial institutions to remove employees upon termination and periodically reviewing and recertifying capabilities for 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.[2]

Recommendations—The Office should:

1. Update bank account or investment portfolio documentation to include only authorized employees to safeguard public monies.
2. Develop and implement policies and procedures to:
   a. Immediately prepare formal written communications or complete required forms to request the banking or investing financial institutions to remove all capabilities for former employees and update all documentation to include only authorized employees.
   b. Review banking or investing financial institutions documentation listings immediately after requesting the institution to remove capabilities to verify that only authorized users remain.
   c. Periodically review and recertify authorized employees' capabilities related to bank accounts and investment portfolios.

The Office'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] Three of 4 bank accounts were the same accounts included in the previously mentioned 8 bank accounts.

[2] U.S. Government Accountability Office (GAO). (2014). Standards for internal control in the federal government. Washington, DC. Retrieved 9/10/2024 from https://www.gao.gov/assets/670/665712.pdf

2024-02

The Office of the Arizona State Treasurer's (Office) control procedures over IT systems and data were not sufficient, which increases the risk that the Office may not adequately protect those systems and data

Condition—Contrary to its policies and procedures in effect at the time, the Office did not document and implement some control procedures to respond to risks associated with its IT systems and data. Specifically, the Office's inconsistency or lack of documentation and implementation may not have prevented risks in the following areas:

- **Managing system configurations and changes—**Procedures did not ensure configuration settings were securely maintained and all IT system changes were adequately managed.
- **Ensuring operations continue—**Contingency plan was not tested to ensure the Office could restore operations in the event of a disaster or other system interruption.

Effect—There is an increased risk that the Office 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 Office'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 Office's administration and IT management reported that it did attempt to follow policies and procedures requiring it to respond to risks associated with its IT systems and data but because of limited resources and timing between audits, they were unable to correct these previously reported findings. These policies were commensurate with the State of Arizona's IT policies established by the Arizona Strategic Enterprise Technology Office (ASET) in effect at the time of policy implementation for addressing the risks associated with its IT systems.

Criteria—The Office is required to follow the State's IT policies ASET established to implement effective internal controls that 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:

- **Manage system configurations and changes through well-defined, documented configuration management process—**Ensures the Office'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.
- **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—The Office should:

1. Follow the State of Arizona's IT policies established by ASET to:
   a. Document, implement, and monitor compliance with its IT policies and procedures and develop a process to ensure the procedures are being consistently followed.
   b. Work with ASET on the ways to implement audit recommendations.

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

2. Establish and follow a documented change-management process.
3. Review proposed changes for appropriateness, justification, and security impact.
4. Document changes, testing procedures, and results.
5. Test changes prior to implementation.
6. Maintain configurations for all system services, assets, and infrastructure; manage configuration changes; and monitor the system for unauthorized or unintended configuration changes.

Ensure operations continue—To ensure operations continue update, document, and implement processes to:

7. Test the contingency plan.

The Office'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.

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

TREASURER RESPONSE

OFFICE OF THE
ARIZONA STATE TREASURER

KIMBERLY YEE
TREASURER

May 9, 2025

Lindsey A. Perry
Arizona Auditor General
291 N. 44th St., Ste. 410
Phoenix, AZ 85018

Dear Ms. Perry:

We have prepared the 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 the name of the contact person responsible for the corrective action, the anticipated completion date, our opinions and view, and the corrective action plan.

Sincerely,

Jackie Harding

Jackie Harding
Deputy Treasurer of Operations

2024-01

Agency: Arizona State Treasurer's Office
Name of Contact Person and Title: Jackie Harding, Deputy Treasurer of Operations
Anticipated Completion Date: June 30, 2025
Agency Response: Concur

OFFICIAL VIEW/OPINION

Under no circumstances may any employee, whether current or former, have complete and independent access to perform banking or investment transactions that remove funds from the state's possession because of the comprehensive protocols that are in place to prohibit any activity by only one person.

All Treasury accounts, including those listed in the report, require elevated security verification requirements and have well-established internal controls that prohibit one signer, even current authorized employees, from performing transactions that would cause monies to be moved out of the State's accounts. No current or former employee who is a signer on any of these accounts can independently perform "in and out" transactions, including withdrawals.

A few of the established security measures include:

- Due to high level security measures, there is an inability to perform banking transactions at a financial institution, including signers of the accounts.
- Two employees, at minimum, are required to perform transactions where funds are sent out of the state. This process can only be performed through the bank's secure portal.
- When changes are made to authorized personnel, the financial institutions administer live callback verifications to ASTO employees via phone prior to updating authorized personnel.
- There are limited capabilities that prohibit check activity, withdrawals, and in-person transactions from being performed.

All banking and financial partners were timely made aware of the employees who were no longer with the Treasurer's Office and the State of Arizona through email, telephone conversations or both. If such personnel notifications are provided by our office with good intent, and the external partner institution does not send our office the documents to complete and update, then it is difficult to know what the partnering financial institution expects or requires of the paperwork. Our office maintains a very close relationship with all of our banking and investment partners and continuously keeps them updated on any changes that would affect financial operations, including personnel changes. The accounts are consistently monitored and reconciled to the statewide accounting system and there have not been any fraudulent transactions performed or attempted.

CORRECTIVE ACTION PLAN

To ensure that financial documentation is updated timely, we are working on developing internal documented policies, procedures and checklists to ensure that the financial institution documents are updated and reviewed periodically (at least annually) for accuracy. We will continue to work closely with our banking and investment partners to ensure that they have the proper and most up-to-date services on our accounts that will continue to prevent unauthorized transactions and safeguard the office.

2024-02

Agency: Arizona State Treasurer's Office
Name of Contact Person and Title: Jackie Harding, Deputy Treasurer of Operations
Anticipated Completion Date: June 30, 2025
Agency Response: Concur

OFFICIAL OPINION/VIEW

The Treasurer's Office stives to maintain a strong security posture that meets or in some cases exceeds the IT-security requirements in state policy. Office staff are committed and dedicated to protecting state and citizen data and will continue to secure that information to prevent unauthorized or inappropriate access to systems so that operations can continue during outages. We also would like to note that there hasn't been any unauthorized or inappropriate access to our systems and all systems are secure.

ACTION PLAN

The Treasurer's Office strives to consistently maintain a strong IT security posture that protects state and citizen data. ASTO has been and will continue to rely on the Arizona Department of Homeland Security guidelines and guidance. We remain committed to protecting state and citizen data, and to providing secure and efficient technologies for our agency. We are taking steps to protect our systems and data while continuing to focus on documentation practices that align with the statewide policy and performing regular testing of the policies and recovery methods documented.


ARIZONA
Auditor General
Making a Positive Difference