Office of the Arizona State Treasurer

Report on Internal Control and on Compliance

Year Ended June 30, 2023

A Report to the Arizona Legislature

Lindsey A. Perry
Auditor General

ARIZONA
Auditor General
Making a Positive Difference

ARIZONA
AuditorGeneral
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

Representative **Matt Gress**, Vice Chair
Representative **Tim Dunn**
Representative **Alma Hernandez**
Representative **Beverly Pingerelli**
Representative **Marcelino Quiñonez**
Representative **Ben Toma** (ex officio)

Senator **Sonny Borrelli**, Chair
Senator **David C. Farnsworth**
Senator **Anthony Kern**
Senator **Juan Mendez**
Senator **Catherine Miranda**
Senator **Warren Petersen** (ex officio)

Audit Staff

Melanie M. Chesney, Deputy Auditor General and Acting Director, Financial Audit Division
Don Bohart, 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 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, 2023, 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, 2023.

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.

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. 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 2023-01 and 2023-02, that we consider to be significant deficiencies.

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, and contracts, 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*.

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, 2023

SCHEDULE OF FINDINGS AND RECOMMENDATIONS

Financial statement findings

2023-01

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

Effect—The Office's operations, IT systems, and data may have been at unintended and unnecessary risk of potential harm.

Cause—The Office's administration and IT management reported that it did not review its entity-wide IT risks, or identify, classify, and inventory sensitive information that might need stronger access and security controls because it did not follow its own documented policies and procedures. 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 that ASET established to help effectively manage risk at the Office and within its IT systems. Effectively managing risk includes an entity-wide risk assessment process that involves members of the Office's administration and IT management. An effective risk assessment process helps the Office determine the risks it faces as the Office 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. Additionally, an effective risk management process provides the Office with 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 Office's objectives can be met, an effective annual risk assessment considers and identifies IT risk in the Office's operating environment, analyzes and prioritizes each identified risk, and develops a plan to respond to each risk within the context of the Office's defined objectives and risk tolerances. Finally, effectively managing risk includes the Office'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—The Office's administration and IT management should follow the State of Arizona's IT policies established by the Arizona Strategic Enterprise Technology Office (ASET) to:

1. Identify, analyze, and reduce risks to help prevent undesirable incidents and outcomes that could impact business functions and IT systems and data.
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 Office holds to assess where stronger access and security controls may be needed to protect data in accordance with State statutes and federal regulations.

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.

2023-02

The Office of the Arizona State Treasurer's 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 of the Arizona State Treasurer (Office) did not document and implement 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:

- **Access—**May not have helped prevent or detect unauthorized or inappropriate access to its IT systems and data.
- **System configurations and changes—**Configuration settings may not have been securely maintained and all IT system changes may not have been adequately managed.
- **Security of systems and data—**Controls may not have prevented unauthorized or inappropriate access or use, manipulation, damage, or loss.
- **Ensure operations continue—**Contingency plan lacked key elements related to restoring operations in the event of a disaster or other system interruption.

Effect—The Office's IT systems and data were at increased risk of unauthorized or inappropriate access, which could result in compromising or the loss of information or integrity of systems and data. The Office was also at increased 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 not follow its policies and procedures requiring it to respond to risks associated with its IT systems and data. 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 that 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:

- **Restrict 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.
- **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.
- **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.
- **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's administration and IT management should follow the State of Arizona's IT policies established by the Arizona Strategic Enterprise Technology Office (ASET) to:

1. Document, implement, and monitor compliance with its IT policies and procedures and develop a process to ensure the procedures are being consistently followed.
2. Work with ASET on ways to implement audit recommendations.

Restrict access—To restrict access to its IT systems and data, update, document, and implement processes to:

3. Assign and periodically review employee user access ensuring appropriateness and compatibility with job responsibilities.

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

4. Establish and follow a documented change management process.
5. Document review of proposed changes for appropriateness, justification, and security impact.
6. Document testing procedures, results and change approvals.
7. Develop and document a plan to roll back changes in the event of a negative impact to IT systems.
8. Document testing of changes prior to implementation.
9. Separate responsibilities for the change management process or, if impractical, perform a post-implementation review to ensure the change was implemented as approved.

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

10. Update and implement a security incident response plan clearly stating how to report and handle such incidents.
11. Ensure awarding and subsequent monitoring of IT vendor contracts is adequately conducted to ensure vendor qualifications and adherence to the vendor contract.

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

12. Update the contingency plan, and ensure it includes all critical elements to restore critical operations.
13. Test the contingency plan.
14. Train staff responsible for implementing the contingency plan.
15. Securely maintain and test backups of systems and data.

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.

TREASURER RESPONSE

OFFICE OF THE

ARIZONA STATE TREASURER

KIMBERLY YEE
TREASURER

December 15, 2023

Lindsey A. Perry
Arizona Auditor General
291 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. 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,

Mark Swenson

Deputy Treasurer

Arizona State Treasurer’s Office

Corrective Action Plan
Year Ended June 30, 2023

2023-01

Agency: Arizona State Treasurer’s Office
Name of contact person and title: Jackie Harding, Deputy Treasurer, Operations
Anticipated completion date: June 30, 2024
Agency Response: Concur

The Treasurer’s Office maintains a strong security posture that meets or exceeds the IT-security criteria outlined in state policy in many areas. We remain committed to protecting state and citizen data, and to providing secure and efficient technologies for our agency. We note that there was no unauthorized or inappropriate access to our systems. And to be clear, we believe that our IT systems are secure, and we do not believe that our IT practices have put any data or operations at risk.

While we believe we currently have proper operational controls in place, including existing ASTO policies and procedures that comply with the Arizona Department of Homeland Security’s guidance, we recognize the importance of policy and procedural documentation to support them. We are committed to ensuring that internal documentation reiterates the other agencies’ guidance and confirms on-going compliance. To that end, the Treasurer’s Office is working internally to develop and implement an updated internal plan related to identifying, evaluating, and documenting parallel Arizona Department of Homeland Security’s guidance, or that otherwise meets or exceeds state policy. The Treasurer’s Office also intends to conduct an annual entity-wide risk assessment, consistent with the Auditor General’s recommendations.

Additionally, we have identified internal tools at our disposal that we can use to create a robust data classification system. We intend to implement that system by June 30, 2024.

2023-02

Agency: Arizona State Treasurer’s Office
Name of contact person and title: Jackie Harding, Deputy Treasurer, Operations.
Anticipated completion date: June 30, 2024
Agency Response: Concur

Again, the Treasurer’s Office consistently maintains a strong security posture that meets or exceeds the IT-security criteria outlined in state policy in many areas. ASTO has been relying and will continue to rely on the Arizona Department of Homeland Security’s guidelines in this area. Based on this finding, we appreciate the need to reiterate the existing guidance in a separate ASTO policy. We remain committed to protecting state and citizen data, and to providing secure and efficient technologies for our agency. And we note once more that there was no unauthorized or inappropriate access to our systems. Those systems are secure.

Nevertheless, the Treasurer’s Office is currently working to bring all policy and procedural documentation in line with Arizona Department of Homeland Security’s separate policies, rather than just relying on those separate policies in its operations. This update will ensure that the documentation reflects our current technologies and processes. We have also already begun the process of reviewing staff access, updating the appropriate documentation to reflect the Auditor General’s recommendations, and making operational adjustments where needed. This includes ensuring that up-to-date, internally documented processes are in place for a contingency plan and security incident response rather than relying solely on the Arizona Department of Homeland Security’s guidance on responses.

Finally, we have identified and already implemented a solution for a change management process that also includes approval mechanisms. These changes will bolster the Treasurer’s Office’s already-secure IT systems and operations.

ARIZONA
Auditor General
Making a Positive Difference