

Pima County

Report on Internal Control
and on Compliance

Year Ended June 30, 2018



A Report to the Arizona Legislature

Lindsey A. Perry
Auditor General





The Arizona Office of the Auditor General's mission is to provide independent and impartial information and specific recommendations to improve the operations of State and local government entities. To this end, the Office provides financial audits and accounting services to the State and political subdivisions, investigates possible misuse of public monies, and conducts performance audits and special reviews of school districts, State agencies, and the programs they administer.

The Joint Legislative Audit Committee

Senator **Rick Gray**, Chair
Senator **Lupe Contreras**
Senator **Andrea Dalessandro**
Senator **David C. Farnsworth**
Senator **David Livingston**
Senator **Karen Fann** (ex officio)

Representative **Anthony T. Kern**, Vice Chair
Representative **John Allen**
Representative **Timothy M. Dunn**
Representative **Mitzi Epstein**
Representative **Jennifer Pawlik**
Representative **Rusty Bowers** (ex officio)

Audit Staff

Donna Miller, Director
John Faulk, Manager and Contact Person

Contact Information

Arizona Office of the Auditor General
2910 N. 44th St.
Ste. 410
Phoenix, AZ 85018

(602) 553-0333

www.azauditor.gov



TABLE OF CONTENTS

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 <i>Government Auditing Standards</i>	1
Schedule of findings and recommendations	3
Financial statement findings	3
County response	
Corrective action plan	
Report issued separately	
Comprehensive Annual Financial Report	



MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

ARIZONA AUDITOR GENERAL
LINDSEY A. PERRY

JOSEPH D. MOORE
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 Board of Supervisors of
Pima 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 Comptroller General of the United States, the financial statements of the governmental activities, business-type activities, discretely presented component unit, each major fund, and aggregate remaining fund information of Pima County as of and for the year ended June 30, 2018, 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 19, 2018. Our report includes a reference to other auditors who audited the financial statements of the Stadium District, School Reserve Fund, Wireless Integrated Network, Self-Insurance Trust, Health Benefit Trust, Regional Wastewater Reclamation Department, Development Services, and Southwestern Fair Commission, 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.

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) to determine the 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 have not been 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 did identify certain deficiencies in internal control, described in the accompanying schedule of findings and recommendations as items 2018-01 and 2018-02, that we consider to be significant deficiencies.

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 determination of financial statement amounts. 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 and those of the other auditors disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

Pima County response to findings

Pima County's responses to the findings identified in our audit are presented in its corrective action plan at the end of this report. The County's responses were not subjected to the auditing procedures applied in the audit of the basic financial statements, and accordingly, we express no opinion on them.

Purpose of this report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the 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.

Donna Miller, CPA
Director, Financial Audit Division

December 19, 2018



SCHEDULE OF FINDINGS AND RECOMMENDATIONS

Financial statement findings

2018-01

Managing risk

Condition and context—The County’s process for managing risks involved some departments responsible for performing their own risk assessments, such as the Treasurer’s Office (Treasurer), and did not include an overall risk-assessment process that included identifying, analyzing, and responding to the County-wide information technology (IT) risks, such as potential harm from unauthorized access, use, disclosure, disruption, modification, or destruction of IT data and systems. Also, it did not include identifying, classifying, and inventorying sensitive information that might need stronger access and security controls. Finally, it did not include evaluating and determining the business functions and IT systems that would need to be restored quickly if the County or any of its departments, such as the Treasurer, were impacted by disasters or other system interruptions.

Criteria—Effectively managing risk at the County includes an entity-wide risk-assessment process that involves members of the County’s administration and IT management to determine the risks the County faces as it seeks to achieve its objectives to not only report accurate financial information and protect its IT systems and data but to also carry out its overall mission and service objectives. The process should provide the basis for developing appropriate responses based on identified risk tolerances and specific potential risks to which the County might be subjected. To help ensure the County’s objectives can be met, an annual risk assessment should include considering IT risks. For each identified risk, the County should analyze the identified risk and develop a plan to respond within the context of the County’s defined objectives and risk tolerances. The process of managing risks should also address the risk of unauthorized access and use, modification, or loss of sensitive information and the risk of losing the continuity of business operations in the event of a disaster or system interruption.

Effect—The County’s and Treasurer’s administration and IT management may put their operations and IT systems and data at unintended and unnecessary risk.

Cause—The County and Treasurer have relied on an informal process to perform risk-assessment procedures that did not include IT security.

Recommendations—The County and Treasurer should identify, analyze, and reduce risks to help prevent undesirable incidents and outcomes that could impact business functions and IT systems and data. They also should plan for where resources should be allocated and where critical controls should be implemented. To help ensure they have effective entity-wide policies and procedures to achieve these objectives, the County and Treasurer should follow guidance from a credible IT security framework such as that developed by the National Institute of Standards and Technology. Responsible administrative officials and management over finance, IT, and other entity functions should be asked for input in the County’s and

Treasurer's process for managing risk. The County and Treasurer should conduct the following as part of their process for managing risk:

- Perform an annual, entity-wide IT risk-assessment process that includes evaluating risks such as risks of inappropriate access that would affect financial data, system changes that could adversely impact or disrupt system operations, and inadequate or outdated system security.
- Evaluate and manage the risks 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. (County only)
- Evaluate and determine the business functions and IT systems that would need to be restored quickly given the potential impact disasters or other IT system interruptions could have on critical organizational functions, such as public safety and operations, such as payroll and accounting, and determine how to prioritize and plan for recovery.

The County's and Treasurer's responsible officials' views and planned corrective action are in their corrective action plan included at the end of this report.

This finding is similar to prior-year finding 2017-01.

2018-02

Information technology (IT) controls—access, configuration and change management, security, and contingency planning

Condition and context—The County sets policies and oversees control procedures for most of its departments' IT operations, systems, and data except for certain departments, such as the Treasurer's Office (Treasurer). The County's and Treasurer's control procedures were not sufficiently designed, documented, and implemented to respond to risks associated with their IT systems and data. The County and Treasurer, as applicable, lacked adequate procedures over the following:

- **Restricting access to its IT systems and data**—Procedures did not consistently help prevent or detect unauthorized or inappropriate access.
- **Configuring systems securely and managing system changes**—Procedures did not ensure IT systems were securely configured and all 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.
- **Updating a contingency plan**—Plan lacked key elements related to restoring operations in the event of a disaster or other system interruption.

Criteria—The County and Treasurer should have effective internal controls to protect their IT systems and help ensure the integrity and accuracy of the data they maintain.

- **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.
- **Well-defined documented configuration management process**—Ensures the Treasurer's IT systems are configured securely 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 security or operations. Separation of 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.

- **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 IT systems and data.
- **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.

Effect—There is an increased risk that the County and Treasurer may not adequately protect their IT systems and data, which could result in unauthorized or inappropriate access and the loss of confidentiality and integrity of systems and data. It also increases the County's and Treasurer'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 and Treasurer continue to develop and review their written policies and procedures over IT access, configuration and change management, security, and contingency planning; however, many of the policies and procedures are still lacking critical elements to ensure they are comprehensive and effective.

Recommendations—To help ensure the County and Treasurer have effective policies and procedures over their IT systems and data, the County and Treasurer should follow guidance from a credible IT security framework such as that developed by the National Institute of Standards and Technology. To help achieve these control objectives, the County and Treasurer should develop, document, and implement control procedures in each applicable IT control area described below:

Access

- Assign and periodically review employee user access ensuring appropriateness and compatibility with job responsibilities.
- Review all other account access to ensure it remains appropriate and necessary.
- Evaluate the use and appropriateness of accounts shared by 2 or more users and manage the credentials for such accounts.
- Enhance authentication requirements for IT systems.
- Manage employee-owned and entity-owned electronic devices connecting to systems and data.
- Manage remote access to systems and data.

Configuration and change management (Treasurer only)

- Establish and follow a documented change management process.
- Review proposed changes for appropriateness, justification, and security impact.
- Document changes, testing procedures and results, change approvals, and post-change review.
- Develop and document a plan to roll back changes in the event of a negative impact to IT systems.
- Test changes prior to implementation.
- Separate responsibilities for the change management process or, if impractical, perform a post-implementation review to ensure the change was implemented as approved.
- Configure IT resources appropriately and securely and maintain configuration settings.

Security

- Perform proactive key user and system activity logging and log monitoring, particularly for users with administrative access privileges. (Treasurer only)

- Prepare and implement a security-incident-response plan clearly stating how to report and handle incidents.
- Provide all employees ongoing training on IT security risks and their responsibilities to ensure systems and data are protected.
- Perform IT vulnerability scans and remediate vulnerabilities in accordance with a remediation plan.
- Identify, evaluate, and apply patches in a timely manner. (Treasurer only)
- Develop, document, and follow a process for awarding IT vendor contracts. (County only)

Contingency planning

- Update the contingency plan and ensure it includes all required elements to restore critical operations, including being prepared to enable moving critical operations to a separate alternative site if necessary.
- Test the contingency plan.
- Train staff responsible for implementing the contingency plan.

The County's and Treasurer's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

This finding is similar to prior-year findings 2017-02 (access), 2017-03 (configuration and change management), 2017-04 (security), and 2017-05 (contingency planning).

COUNTY RESPONSE



January 25, 2019

Lindsey 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*. 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,

Michelle Campagne, Director
Finance and Risk Management

Michelle Campagne, Director

130 W Congress, 6th Fl Tucson, Arizona 85701-1317 • Phone: 520-724-8410 • Fax: 520-770-4173

Pima County
Corrective action plan
Year ended June 30, 2018

Financial statement findings

2018-01

Managing risk

Name of contact person: Dan Hunt, CIO and Beth Ford, Treasurer

Anticipated completion date: June 30, 2020

The County agrees with the finding and recommendations. The County is currently drafting procedures and will perform an IT security risk assessment as part of the overall County risk assessment process that identifies risk scenarios, including the scenarios' likelihood and magnitude; documentation and dissemination of results; review by appropriate personnel; and prioritization of risks for remediation. This process includes identifying what the County classifies as sensitive information and the steps taken to inventory and protect it.

The Pima County Treasurer's Office (PCTO) has contracted with an outside firm for a complete risk assessment of its systems and procedures to be completed by the end of fiscal year 2019. The PCTO will use the results of the risk assessment to determine and prioritize the corrective action required.

2018-02

Information technology (IT) controls—access, configuration and change management, security, and contingency planning

Name of contact person: Dan Hunt, CIO and Beth Ford, Treasurer

Anticipated completion date: June 30, 2019

The Information Technology Department (ITD) is currently updating its system access procedures to require additional documentation that demonstrates the County procedures are being followed. ITD is also coordinating with departments to ensure system access is appropriate and accounts with elevated privileges are monitored and reviewed periodically. In addition, security related items will be addressed by procedures currently being drafted for incident response, ongoing security training for employees, and vulnerability scanning with remediation actions. Finally, ITD will work with the departments to update the County's contingency plan.

The PCTO has contracted with an outside firm for a complete risk assessment of its systems and procedures to be completed by the end of fiscal year 2019. The PCTO will use the results of the risk assessment to determine and prioritize the corrective action required. ITD will be available to assist the PCTO with remediation of configuration, change management, and contingency planning issues.

