A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Report on Internal Control and Compliance

Pima County

Year Ended June 30, 2015

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

Debra K. Davenport
Auditor General

The **Auditor General** is appointed by the Joint Legislative Audit Committee, a bipartisan committee composed of five senators and five representatives. Her mission is to provide independent and impartial information and specific recommendations to improve the operations of state and local government entities. To this end, she provides financial audits and accounting services to the State and political subdivisions, investigates possible misuse of public monies, and conducts performance audits of school districts, state agencies, and the programs they administer.

The Auditor General's reports are available at:

www.azauditor.gov

Printed copies of our reports may be requested by contacting us at:

Office of the Auditor General
2910 N. 44th Street, Suite 410 • Phoenix, AZ 85018 • (602) 553-0333

Pima County
Report on Internal Control and Compliance
Year Ended June 30, 2015

Table of Contents

Report Issued Separately

Comprehensive Annual Financial Report

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
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 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, 2015, 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 3, 2015. Our report includes a reference to other auditors who audited the financial statements of the Stadium District, School Reserve Fund, Office of Emergency Management's Radio System, 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.

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 over financial reporting that we consider to be a material weakness 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 County's basic 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 2015-01 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 deficiencies described in the accompanying Schedule of Findings and Recommendations as items 2015-02 through 2015-04 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 on pages 9 and 10. 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.

Jay Zsorey, CPA
Financial Audit Director

December 3, 2015

Pima County
Schedule of Findings and Recommendations
Year Ended June 30, 2015

Financial Statement Findings

2015-01

The County should improve security over its information resources

Criteria: To effectively maintain and secure financial and sensitive information, the County should establish internal control policies and procedures that include practices to help prevent, detect, and respond to instances of unauthorized access or use, manipulation, damage, or loss to its information technology (IT) resources that are based on acceptable IT industry practices. The County's IT resources include its systems, network, infrastructure, and data.

Condition and context: The County did not:

- Develop a county-wide IT security risk-assessment process.
- Identify and categorize data by sensitivity and take appropriate action to protect sensitive information. For example, auditors discovered sensitive information on a county change management document that was unsecured and potentially accessible by county employees.
- Proactively log and monitor key user and system security activity. While the County has a process for logging and monitoring systems, this process is not formally documented, and many logs are not reviewed on a proactive basis but only as issues arise.
- Manage remote access security risks for both the County's network and individual users. Remote access allows users to access network resources from locations other than county buildings.
- Require appropriate security measures for employee-owned electronic devices with access to the County's network.
- Manage the installation of software on employee workstations. For example, the County had no written policy or process to monitor and detect unauthorized software.
- Establish a process to identify and respond to security incidents.
- Assess the security risks associated with using outdated and unsupported software or take steps to secure the software. This software potentially contains vulnerabilities because the vendor no longer provides security updates to protect against malicious attacks.
- Provide continuous training to keep IT personnel up to date on IT security risks, controls, and practices. In addition, the County did not have a security awareness program for its employees, nor did it have a training program to help ensure they were familiar with the County's IT security policies and procedures.
- Have an adequate process to identify vulnerabilities in its IT resources.
- Have an adequate process or documented policies and procedures to ensure patches are applied to all IT resources.
- Have a process in place to ensure its IT resources are configured securely.
- Properly manage its IT vendors and cloud service contracts.
- Have a policy or process for protecting digital and non-digital media.

Effect: There is an increased risk that the County may not prevent or detect unauthorized access or use, manipulation, damage, or loss to its IT resources.

Cause: The County was unaware its policies and procedures lacked critical elements related to IT security and did not evaluate its written policies and procedures against current IT standards and best practices.

Recommendation: To help ensure that the County is able to effectively maintain and secure its IT resources, the County should ensure that its policies and procedures over securing its IT resources are documented in writing, implemented, and include the following:

- Conducting an IT security risk-assessment process when there are changes to the IT resources or at least annually that includes identification of risk scenarios that could impact the County, including the scenarios' likelihood and magnitude; documentation and dissemination of results; review by appropriate personnel; and prioritization of risks for remediation. Also, incorporate any threats identified as part of the County's IT security vulnerability scans into the IT security risk-assessment process.
- Identifying, categorizing, and inventorying sensitive information and developing security measures to protect it, such as implementing controls to prevent unauthorized access to the information. The County's policies and procedures should include the security categories into which information should be classified as well as the state statutes and federal regulations that impact those categories.
- Performing proactive logging and log monitoring. The County should log key user and system activity, particularly users with administrative access privileges and remote access, along with other activities that could result in potential security incidents such as unauthorized access. The County should determine what events to log, configure the system to generate the logs, and decide how often to monitor these logs for indicators of potential attacks or misuse of IT resources. Also, the County should maintain activity logs where users with administrative access privileges cannot alter them.
- Managing remote access by requiring that security controls be utilized for all remote access. These controls should include the appropriate configuration of security settings such as configuration/connection requirements; the use of encryption to protect the confidentiality and integrity of remote sessions; the routing of all remote access through a secure channel; the approval of administrative access privileges; remote access only for purposes defined, documented, and justified in the County's remote access policy; and the ability to quickly disconnect or disable remote access. In addition, remote access should be actively monitored to detect cyber-attacks and ensure compliance with remote access policies.
- Managing employee-owned electronic devices connecting to the network, including specifying security configuration requirements while on the County's network.
- Managing software installed on employee computer workstations. Policies and procedures should address what software is appropriate and the process for requesting, approving, installing, monitoring, and removing software on employee computer workstations.
- Establishing and documenting a process to identify and respond to security incidents. This process should include developing and testing an incident response plan and training staff responsible for the plan. The plan should define reportable incidents and address steps on how to identify and handle incidents that include preparation, detection and analysis, containment, eradication, and recovery. The plan should also coordinate incident handling activities with contingency-planning activities, and incorporate lessons learned from ongoing incident handling into the incident response procedures. The incident response plan should be distributed to incident response personnel and updated, as necessary. Suspected incidents should be reported to incident response personnel so incidents can be tracked and documented. The County should also ensure these policies and procedures follow regulatory and statutory requirements, provide a mechanism for assisting users in handling and reporting security incidents, and include making disclosures to affected individuals and appropriate authorities should an incident occur.

- Implementing a strategy for assessing and securing any software that the manufacturer no longer updates and supports.
- Developing a plan to provide continuous training on IT security risks, controls, and practices for the County's IT personnel. In addition, the County should develop a security awareness training program for all employees that provides a basic understanding of information security, user actions to maintain security, and how to recognize and report potential indicators of security threats, including threats generated by other county employees. Such training should be provided for new users and on an on-going basis as determined by the County.
- Developing a formal process for vulnerability scans that includes performing IT vulnerability scans on a periodic basis and utilizing tools and techniques to automate parts of the process by using standards for software flaws and improper configuration, formatting procedures to test for the presence of vulnerabilities, and measuring the impact of identified vulnerabilities. In addition, the County should analyze vulnerability scan reports and results, remediate legitimate vulnerabilities as appropriate, and share information obtained from the vulnerability-scanning process with county departments to help eliminate similar vulnerabilities.
- Finalizing and implementing the County's patch management policies and procedures to ensure patches are evaluated, tested, and applied in a timely manner once the vendor makes them available.
- Configuring IT resources to provide only essential capabilities to help prevent unauthorized connection of devices or transfer of information. The County should review IT resources' functions and services to determine which functions and services it should eliminate.
- Developing a process to consider IT risks, costs, benefits, and technical specifications prior to awarding IT vendor contracts. In addition, the County should ensure contracts include specifications addressing the management, reliability, governance, and security of the County's IT resources. Finally, for cloud services, the County should ensure service contracts address all necessary security requirements based on best practices, such as physical location of data centers. The County should also monitor the IT vendors' performance to ensure conformance with county contracts.
- Developing media protection policies and procedures to restrict access to media containing data the County, federal regulation, or state statute identifies as sensitive or restricted. Such policies and procedures should require that the County appropriately mark media indicating the distribution limitations and handling criteria for data included on the media. In addition, the County should physically control and secure such media until it can destroy or sanitize it using sanitization mechanisms with the strength and integrity consistent with the information's security classification.

2015-02

The County should improve access controls over its information technology resources

Criteria: The County should have effective internal control policies and procedures to control access to its IT resources.

Condition and context: The County did not have adequate policies and procedures in place to limit logical access to its IT resources. Specifically, the County did not periodically perform reviews of user access, group accounts, or logs to:

- Ensure access was needed and compatible with employees' job responsibilities.
- Evaluate the appropriateness of remote access rights, which allow users to access its network from locations other than county buildings.
- Remove access rights for terminated employees.
- Ensure generic accounts are appropriately limited.
- Monitor users, especially those with elevated system access.
- Re-issue group account credentials as individuals were removed from the group.

In addition, the County did not require all network account passwords to be reset after 60 days, as required by county policy, and allowed for some passwords to never expire. Further, county policies and procedures did not require a lockout of network accounts after several consecutive unsuccessful login attempts.

Effect: There is an increased risk that the County may not prevent or detect unauthorized access or use, manipulation, damage, or loss of IT resources, including sensitive and confidential information.

Cause: The County does not have sufficient policies and procedures and lacked detailed instructions for employees to follow for granting and reviewing access to its IT resources.

Recommendation: To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the County should establish and implement effective policies and procedures that include the following:

- Performing a periodic, comprehensive review of all existing employee access accounts to help ensure that network and system access granted is needed and compatible with job responsibilities.
- Reviewing remote access rights to determine if the access is necessary and appropriate.
- Removing employees' network and systems access immediately upon their terminations.
- Reviewing all generic accounts on its network and systems to eliminate or minimize their use where possible.
- Reviewing and monitoring the activity of users with elevated access for propriety.
- Monitoring and re-issuing account credentials on group accounts when a group member leaves.
- Strengthening network password policies by requiring users to change passwords on a periodic basis and by developing a reasonable account lockout threshold for incorrect password attempts.

2015-03

The County should improve its information technology change management processes

Criteria: The County should have adequate change management internal control policies and procedures to track and document changes made to its IT resources.

Condition and context: The County's written policies and procedures for managing changes to its IT resources lacked critical elements. Specifically:

- The County's policies and procedures did not require a security impact analysis to assess changes' impact or require documentation of whether all changes had met security requirements prior to implementation.
- The County's policies and procedures did not require sufficient documentation of change testing procedures and results for changes made. Auditors noted approved changes with no documentation of test procedures performed or test results.
- The County lacked policies and procedures for emergency changes to its financial systems.

In addition, auditors noted an emergency change that was marked as medium priority rather than critical or high in accordance with county policy.

Effect: There is an increased risk that changes to the County's IT resources could be unauthorized or inappropriate, or could have unintended results without proper documentation, authorization, review, testing, and approval prior to being applied.

Cause: The County was unaware its policies and procedures lacked critical elements and did not evaluate its policies and procedures against current IT standards and best practices.

Recommendation: To help prevent and detect unauthorized, inappropriate, and unintended changes to its IT resources, the County should improve its written change management policies and procedures for managing changes and improve its change management process to address the following:

- Performing and documenting a security impact analysis when the change is requested and ensuring that all security requirements have been met prior to change implementation.
- Documenting all change details, including test procedures, results, and approvals for each change.
- Documenting the change management process for each type of change, including emergency changes, to its financial systems.
- Ensuring all changes to critical IT resources follow its change management process and are appropriately documented and prioritized.

2015-04

The County should improve its disaster recovery plan for its information technology resources

Criteria: It is critical that the County have a comprehensive, up-to-date disaster recovery plan in place to provide for the continuity of operations and to help ensure that vital IT resources can be recovered in the event of a disaster, system or equipment failure, or other interruption.

Condition and context: Auditors reviewed the County's disaster recovery processes and determined it lacked certain key elements for restoring operations, specifically:

- The disaster recovery plan did not include an analysis and prioritization of recovery for key business processes, including acceptable time frames for restoring those processes.
- The plan was not maintained in a secure location to prevent it from being lost, stolen, or subject to unauthorized modification.
- The plan did not address how changes to the plan would be communicated to key personnel responsible for implementing the plan.
- The plan was incomplete as it omitted several important appendices containing procedures necessary to properly implement the plan such as the plan's security procedures, data center reconstructive plan, list of critical applications, and the master production schedule.
- The County did not perform regularly scheduled, comprehensive tests; document test results; and update the plan for any problems noted.
- The plan did not include policies and procedures for regular training of key personnel to ensure staff would be prepared to carry out the plan.

Effect: The County risks not being able to provide for the continuity of operations and recover vital IT resources and data and conduct daily operations in the event of a disaster, system or equipment failure, or other interruption, which could cause inaccurate or incomplete system information and data and expensive recovery efforts.

Cause: The County has some processes in place but lacks a sufficiently documented recovery plan based on current IT standards and best practices to ensure that its disaster recovery efforts can be relied on in the event they are needed.

Recommendation: To help ensure the continuity of the County's operations in the event of a disaster, system or equipment failure, or other interruption, the County should:

- Incorporate the results of its business impact analysis, including recovery objectives, restoration priorities, and metrics, into the disaster recovery plan to evaluate the impact that disasters could have on its critical business processes and revise its disaster recovery plan to include the analysis' results.
- Store the plan in a secure location accessible to those who need to use it, and protect it from unauthorized disclosure and modification.
- Ensure the plan addresses how to communicate changes to key personnel.
- Ensure that its disaster recovery plan is complete and includes all necessary documents to properly implement the plan.
- Develop a process to perform regularly scheduled tests of the disaster recovery plan and document the tests performed and results. This process should include updating and testing the disaster recovery plan at least annually or as changes necessitate, and coordinating testing with other county plans such as its cyber incident response and emergency response plans. Plan testing may include actual tests, simulations, or table top discussions and should be comprehensive enough to evaluate whether the plan can be successfully carried out. Use test results to update or change the plan.
- Develop and implement an ongoing training schedule for staff responsible for implementing the plan. In addition, ensure training is specific to the users' assigned roles and responsibilities and provided when the plan changes.

COUNTY RESPONSE

PIMA COUNTY

DEPARTMENT OF FINANCE AND RISK MANAGEMENT

February 1, 2016

Ms. Debbie Davenport, Auditor General
State of Arizona, Office of the Auditor General
2910 North 44th Street, Suite 410
Phoenix, AZ 85018

Dear Ms. Davenport:

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 financial reporting finding included in the Report on Internal Control and Compliance we are providing you with the names of the contact persons responsible for corrective action, the corrective action planned, and the anticipated completion timeframe.

Keith Dommer, Director
Finance and Risk Management

Keith Dommer, Finance & Risk Management Director
130 W. Congress, 6th Floor, Tucson, Arizona 85701-1317 Ph: (520)-724-8496 Fax: (520) 770-4173

Pima County
Corrective Action Plan
Year Ended June 30, 2015

Financial Statement Findings

2015-01

The County should improve security over its information resources

Name of contact person: Dan Hunt, Information Security Officer

Pima County agrees with the finding and recommendations. Several points of the recommendation related to policies and procedures are currently being addressed and are expected to be completed in fiscal year 2016-17. For the other points, the County will require additional resources to eliminate the deficiencies. Pima County is in the process of assessing available resources to comprehensively address these issues.

2015-02

The County should improve access controls over its information resources

Name of contact person: Dan Hunt, Information Security Officer

Pima County concurs with the deficiencies and associated recommendations. The County will begin a thorough assessment of all access controls and implement a comprehensive system of monitoring and review based on a continuous risk assessment process. Several access control deficiencies will be remedied in fiscal year 2016-17, and others in the subsequent year.

2015-03

The County should improve its information technology change management process

Name of contact person: Dan Hunt, Information Security Officer

The County agrees with the finding and recommendations. Change management procedures are currently being updated with an expected completion date of July 2016.

2015-04

The County should improve its disaster recovery plan for its information technology resources

Name of contact person: Dan Hunt, Information Security Officer

The County concurs with the finding and the recommendations. Several aspects of the disaster recovery plan will be updated and documented during fiscal year 2016-17, however, many aspects of the plan will require additional resources in subsequent years to complete the plan and assess its effectiveness over time.

Pima County
Report on Internal Control and Compliance
Year Ended June 30, 2015

State of Arizona
Office of the Auditor General