A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Report on Internal Control and Compliance

Coconino 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.

Integrity ★ Accountability ★ Making a Difference ★

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

Coconino 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

DEBRA K. DAVENPORT, CPA AUDITOR GENERAL	OFFICE OF THE 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
Coconino 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, each major fund, and aggregate remaining fund information of Coconino 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 23, 2015.

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 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 County's basic financial statements will not be prevented, or detected and corrected, on a timely basis. We consider the deficiencies described in the accompanying Schedule of Findings and Recommendations as items 2015-01 through 2015-05 to be material weaknesses.

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 2015-06 and 2015-07 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 disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

Coconino County's Response to Findings

Coconino County's responses to the findings identified in our audit are presented on pages 12 through 15. 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 23, 2015

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

Financial Statement Findings

2015-01

The County should follow its procedures when preparing its financial statements and related note disclosures

Criteria: The County's Board of Supervisors and management depend on accurate information to fulfill their oversight responsibilities and to report accurate information to the public and agencies from which the County receives funding. Accordingly, the County should follow its established policies and procedures over financial statement preparation to ensure its financial statements and related note disclosures are accurate, complete, and prepared in accordance with U.S. generally accepted accounting principles (GAAP).

Condition and context: The County did not consistently follow its policies and procedures when preparing its financial statements and related note disclosures. As a result, the County:

- Did not disclose approximately $8.5 million of bank account balances exposed to custodial credit risk.
- Did not use an up-to-date actuarial valuation to measure the other postemployment benefits (OPEB) obligation for its postemployment healthcare plan. While the County used the most recent actuarial valuation available, it was not performed within the minimum frequency of every 2 years as GAAP requires.
- Did not appropriately report pension plan information in its government-wide financial statements and related note disclosures. For example, the County under-reported governmental activities revenues and expenses by $1.2 million related to its proportionate share of the State's appropriation to the Elected Officials Retirement Plan. Further, the notes to the financial statements contained numerous errors. For example, the County under-reported pension expense by $7.4 million, over-reported the annual OPEB cost and contributions made for its agent plans by a combined $2.5 million, and under-reported the sensitivity of the County's net pension liability to changes in the discount rate by a combined $5.7 million.

Effect: The County's financial statements and related note disclosures were not initially prepared in accordance with GAAP. The County made recommended audit adjustments to the financial statements and related note disclosures for all significant errors.

Cause: The County did not thoroughly review the financial statement data and schedules.

Recommendation: The County should follow its established policies and procedures when preparing its annual financial statements and related note disclosures. This will help ensure the County's financial statements and related note disclosures are accurate, complete, and prepared in accordance with GAAP. In addition, the County should improve its procedures by requiring a more detailed review of all data and schedules supporting the financial statements and related note disclosures by someone who is independent of the person preparing the financial statements and is knowledgeable of the County's operations and GAAP reporting requirements.

This finding is similar to prior-year finding 2014-01.

2015-02

The County should separate the responsibilities for managing and operating its financial accounting system

Criteria: No one individual should have full control of the financial accounting system, which includes the information technology hardware, software, and data.

Condition and context: One individual was responsible for managing and operating the County's financial accounting system. Specifically, this individual operated the system's hardware; installed all vendor updates and patches; granted user access to the system; and managed the system's database. Further, this same individual had the ability to process and approve all transactions within the financial accounting system.

Effect: Improper separation of responsibilities increases the risk of errors and irregularities, theft, fraud, and misuse of public monies. In addition, the County risks the ability to ensure the continuity of its daily operations if the individual with overall control of the system is not available.

Cause: The County has not sufficiently trained other employees to perform duties related to managing and operating its financial accounting system.

Recommendation: The County should separate the responsibilities for managing and operating the financial accounting system hardware and software from the responsibilities of managing system data and granting user access and from the abilities to approve, record, and process transactions.

2015-03

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 information technology (IT) resources, which include its systems, network, infrastructure, and data.

Condition and context: The County did not have written policies and procedures to control access to its IT resources. Also, the County did not have an effective process in place for periodically reviewing network and systems' user account access to ensure their access remained necessary and appropriate. As a result, auditors noted that the County allowed terminated employees access to its network and systems, granted an excessive number of systems' user access accounts to vendors, and could not identify all users who had access to its network. In addition, the County did not always require users to have a properly approved access account request form completed prior to granting system access. Further, the County did not effectively log and monitor key activities on its network and systems. Finally, the County did not have effective processes in place for password protection for its network and systems.

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 did not have adequate policies and procedures and lacked detailed instructions for employees to follow for granting and reviewing access to its systems. In addition, the County has various departments that operate the county systems, and not all policies are implemented and communicated county-wide to ensure they are being applied consistently.

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

- Performing a periodic, comprehensive review of all existing employee access accounts to ensure that network and system access granted is needed and compatible with job responsibilities.
- Removing employees' network and systems access immediately upon their terminations.
- Reviewing all vendor access accounts to eliminate or minimize their use when possible.
- Restricting data center access to employees who need it for their job responsibilities and periodically reviewing access granted to ensure that it continues to be needed.
- Documenting all requests and approvals of access granted to its network and systems. Access should be based on the employees' job responsibilities.
- Reviewing and monitoring the key activity of users and those with elevated access for propriety.
- Strengthening network and system password policies by increasing the password length, where applicable, and requiring employees to use complex passwords, change passwords on a periodic basis, and by developing a reasonable account lockout threshold for incorrect password attempts.

2015-04

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 information technology (IT) resources, which include its systems, network, infrastructure, and data.

Condition and context: The County did not have policies and procedures for managing changes to its financial accounting system during the fiscal year. In addition, the County did not have processes in place to ensure that all changes to the financial system were properly documented, authorized, reviewed and tested, and approved prior to implementing them. Finally, the County did not have processes for detecting unauthorized, inappropriate, or unintended changes, and had no post-change process to help ensure that changes were authorized and worked as intended and that no changes circumvented controls.

In addition, auditors reviewed the County's change management policies and procedures for its other critical IT systems managed by the County's IT department and noted the following deficiencies:

- The County did not document testing that was performed on the changes.
- The County did not perform an internal review of the change management process.

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 did not develop written policies and procedures for managing changes to its financial accounting system as it does not typically perform changes to that system. Additionally, the County developed a new change management process during the fiscal year for its other critical IT systems but had not reviewed it to ensure it was consistent with current IT standards and best practices.

Recommendation: To help prevent and detect unauthorized, inappropriate, and unintended changes to its IT resources, the County should establish written policies and procedures for managing changes to its financial accounting system that include the following:

- Establishing a change management process for each type of change, including emergency changes and changes exempt from the change management process. The change management process should include policies and procedures for testing changes and performing an assessment of the security impact of changes prior to implementation.
- Ensuring all changes follow the change management process.
- Reviewing proposed changes to determine appropriateness and justification, considering the security impact for the change.
- Logging, documenting, and retaining records of all change details, including test procedures, results, security impact analysis, and approvals.
- Retaining necessary documentation to support the backing out of changes that negatively impact IT resources.
- Testing changes, including performing a security impact analysis before implementing the change.
- Approving the change at each appropriate phase of the change management process and documenting the approvals.
- Reviewing changes that were implemented to confirm they were implemented as approved and followed the change management process.

Further, the County should improve its written policies and procedures for managing changes and improve the change management processes for its other critical systems managed by the County's IT Department to address the following:

- Documenting the testing of changes, including performing a security impact analysis before implementing the change.
- Reviewing changes that were implemented to confirm they were implemented as approved, and followed the change management process.

2015-05

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 that is performed at least annually, reviewed by appropriate personnel, and includes documentation of results and prioritization of risks for remediation. In addition, any threats identified as part of the County's IT security vulnerability scans should be incorporated into this 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 the County's network that was unsecured and potentially accessible to employees.
- Log and monitor key user and system activity.
- Establish a process to identify and respond to security incidents.
- Have a process in place to ensure its IT resources were configured securely. For example, the County did not limit the functionality of its IT resources to ensure they are performing only essential services.
- Restrict access to IT resources in public areas.
- Establish a security awareness program for its employees and provide continual IT training to keep its IT personnel up to date on IT security risks, controls, and practices.
- Have an adequate process or documented policies and procedures to ensure patches are applied to all IT resources. For example, auditors identified patches that were installed years after their release date.
- Assess the security risks associated with using outdated and unsupported software or take steps to secure the software. Specifically, the County was using outdated and unsupported software that may have been vulnerable because the vendor no longer provided security updates to protect against malicious attacks.
- Have policies and procedures in place for media to ensure sensitive information is handled appropriately when stored or when transferring locations.
- Require all of its employees to sign an acceptable-use agreement.
- Have a process to identify vulnerabilities in its IT resources on a periodic basis, nor did it have a plan to prioritize and remediate or mitigate identified vulnerabilities. For example, various security issues were discovered by auditors during scanning.
- Review, update, and maintain IT policies and procedures. Further, its policies were not formally approved and communicated county-wide.

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 focused its efforts on the day-to-day operations and did not prioritize its IT security policies and procedures or evaluate them 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 identified for remediation. Also, any threats identified as part of the County's IT security vulnerability scans should be incorporated 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 the categories.
- Performing proactive logging and log monitoring. The County should log key user and system activity, particularly users with administrative access privileges and remote user 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.
- 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 security incidents that includes 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 in the incident response procedures. The incident response plan should be distributed to incident response personnel and updated, as necessary. The incident response plan should include provisions for automated incident handling, reporting, and assistance capabilities. Suspected incidents should be reported to individuals responsible for responding 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 make disclosures to affected individuals and appropriate authorities should an incident occur.
- 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.
- Implementing a process to restrict access to IT resources in public areas, including disabling unused Ethernet ports.

- Developing a plan to provide continual 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 to new users and on an ongoing basis as determined by the County.
- Improving its patch management policies and procedures to ensure patches are evaluated, tested, and applied in a timely manner once the vendor makes them available.
- Implementing a strategy for assessing and securing any software that the manufacturer no longer updates and supports.
- 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 caveats given the data included on the media. In addition, the County should physically control and secure such media until it can be destroyed or sanitized using sanitization mechanisms with the strength and integrity commensurate with the information's security classification.
- Adopting an official county-wide acceptable use agreement and have users sign and re-sign on a periodic basis.
- 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 other county departments to help eliminate similar vulnerabilities.
- Reviewing its IT policies and procedures against current IT standards and best practices, and updating them where needed, obtaining the proper authorization, and ensuring policies are implemented county-wide, as appropriate.

2015-06

The County should improve its disaster recovery plan and data backup procedures for its information technology resources

Criteria: It is critical that the County have a comprehensive, up-to-date disaster recovery plan and data backup policies and procedures in place to provide for the continuity of operations and to help ensure that vital information technology (IT) resources, which include its systems, network, infrastructure, and data, can be recovered in the event of a disaster, system or equipment failure, or other interruption.

Condition and context: The County did not have a comprehensive, up-to-date disaster recovery plan in place to provide for the continuity of operations and to help ensure its vital IT resources would be recovered in the event of a disaster, system or equipment failure, or other interruption.

Further, auditors reviewed the County's data backup processes and determined they lacked certain key elements for restoring vital IT resources, specifically:

- The County did not have written policies and procedures, including procedures for restoring its systems using the backup data in an emergency.
- The County did not store their backup data at an off-site location.
- The County did not test its backup data on a regular basis.

Effect: The County risks not being able to provide for the continuity of operations, recovery of 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 had some processes in place but lacked a documented recovery plan based on current IT standards and best practices to ensure that its disaster recovery efforts and backup data could be relied on in the event that 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:

- Conduct a business impact analysis to evaluate the impact disasters could have on its critical business processes. The business impact analysis should identify the County's critical business functions and prioritize the resumption of these services within a time frame acceptable to the County in the event of contingency activation. This business impact analysis' results should be used in developing the County's disaster recovery plan.
- Ensure its disaster recovery plan includes all essential business functions and associated contingency requirements; recovery objectives, restoration priorities, and metrics; contingency roles, responsibilities, and assigned individuals with contact information; identification of critical information assets and processes for migrating to the alternative processing site; processes for eventual system recovery and reconstitution to return the IT resources to a fully operational state and ensure all transactions have been recovered; and review and approval by appropriate personnel. The disaster recovery plan should also be coordinated with incident-handling activities and stored in a secure location, accessible to those who need to use it, and protected from unauthorized disclosure or modification.
- Develop and document procedures for migrating critical information system operations to a separate alternative site for essential business functions. Contracts should be in place or the alternate site should be equipped to resume essential business functions, including provisions for accessibility to the alternate site if necessary. Information security safeguards at the alternative site should be equivalent to the primary site.
- Ensure that its disaster recovery plan is updated for all critical information when changes are made to its IT resources at least annually or as changes necessitate and that the plan addresses how to communicate the changes to key personnel.

- 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 continuity of operations, cyber incident response, and emergency response plans. Plan testing may include actual tests, simulations, or tabletop discussions and should be comprehensive enough to evaluate whether the plan can be successfully carried out. Test results should also be used to update or change the plan.
- Establish and document policies and procedures for testing backups of IT systems and data to help ensure that the County could recover them in the event they are needed. Policies and procedures should require data backups to be protected and stored in an alternative site with security equivalent to the primary storage site. Backups should include user-level information, system-level information, and system documentation, including security-related documentation. In addition, critical information system software and security-related information should be maintained at an alternative site or stored in a fire-rated container.
- Develop and implement an ongoing training schedule for staff responsible for implementing the plan. In addition, ensure training provided is specific to the user's assigned role and responsibilities and provided when the plan changes.

2015-07

The County should follow its policies and procedures over payroll processing

Criteria: The County should have effective internal controls over payroll processing to help ensure employees are paid for only the hours they worked and payroll expenditures are accurately reported in the County's financial statements.

Condition and context: The County's payroll and related expenditures comprised over $68.6 million, or approximately 60 percent, of its total expenditures for the fiscal year ended June 30, 2015. However, the County did not always follow its established policies and procedures over payroll processing by requiring employee time sheets to be reviewed and approved by an appropriate level of management. For example, auditors noted that 2 of 60 time sheets tested were not reviewed and approved.

Effect: Without effective internal controls over payroll processing, the County could inaccurately pay its employees and incorrectly report payroll expenditures in its financial statements. In addition, there is increased risk of fraudulent payroll activity.

Cause: The County's payroll processing is decentralized, and certain departments did not always follow its payroll policies and procedures because of oversight.

Recommendation: To help ensure that county employees are paid for only the hours they work and that payroll expenditures are accurately reported in its financial statements, the County should follow its established policies and procedures over payroll processing and require employee time sheets to be reviewed and approved by an appropriate level of management.

COUNTY RESPONSE

COCONINO
COUNTY ARIZONA

FINANCE

Bonny Lynn
CFO/Director

Heidi Derryberry
Accounting Operations and Special Districts Manager

Jerri Garcia
Financial Management Systems Manager

Tom Johnson
Financial Reporting Audi and Grants Manager

Scott Richardson
Purchasing Manager

Megan Cunningham
Budget and Strategic Planning Manager

February 10, 2016

Debbie Davenport
Auditor General
2910 N. 44th St., Ste. 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.

Sincerely,

Bonny Lynn
Chief Fiscal Officer

219 E. Cherry Ave.
Flagstaff, AZ 86001
928-679-7199

Financial Statement Findings

2015-01

The County should follow its procedures when preparing its financial statements and related note disclosures

Contact Persons: Tom Johnson, Accounting Manager, Finance Department; Bonny Lynn, Finance Director, Finance Department

Anticipated completion date: October 31, 2016

Corrective Action: Concur. The County will modify its financial statement preparation procedures to require a more detailed review of all data and schedules supporting the financial statements and related note disclosures by someone who is independent of the person preparing the financial statements and is knowledgeable of the County's operations and GAAP reporting requirements.

2015-02

The County should separate the responsibilities for managing and operating its financial accounting system

Contact Persons: Jerri Garcia, Financial System Manager; Bonny Lynn, Finance Director, Finance Department

Anticipated completion date: June 30, 2016

Corrective Action: Concur. To ensure that no one individual should have full control of the financial accounting system, the County will work with its software vendors to establish logging and monitoring controls over processing transactions and other activities within the financial accounting system and develop a process for documenting and testing all vendor updates and patches.

In order to ensure continuity of its daily operations, the County has begun training a Sr. Accountant in the Finance Department to perform duties related to managing and operating its financial accounting system.

2015-03

The County should improve access controls over its information technology resources

Contact Person: Kris Estes, IT Director

Anticipated completion date: March 31, 2017

Corrective Action: Concur. To help prevent and detect unauthorized access to IT and unauthorized access or use, manipulation, damage, or loss to its IT systems, including its network, IT infrastructure, system software, and system information and data, the County will continue its efforts to ensure policies and procedures for IT access are documented in writing and are operational.

2015-04

The County should improve its information technology change management processes

Contact Person: Kris Estes, IT Director

Anticipated completion date: March 31, 2017

Corrective Action: Concur. To help prevent and detect unauthorized, inappropriate, and unintended changes to IT systems, including its network, IT infrastructure, system software, and databases, the County will ensure that policies and procedures for change management are documented in writing and are operational.

2015-05

The County should improve security over its information resources

Contact Person: Kris Estes, IT Director

Anticipated completion date: March 31, 2017

Corrective Action: Concur. To help ensure the County's information technology (IT) security is adequate and effective the County will:

- Complete a remediation for vulnerabilities identified as a result of security risk assessments and establish a continual process for assessing IT security risk.

- Perform a comprehensive review of its existing policies and procedures over IT to identify any gaps between the existing policies and procedures, the County's practices and operations, and acceptable practices for IT.

- Develop or update policies and procedures as appropriate.

- Keep IT personnel continuously trained and provide general training to all employees for the appropriate use of IT resources and security awareness.

- Maintain proactive IT security policies and procedures that are documented in writing and are operational.

2015-06

The County should improve its disaster recovery plan and data backup procedures for its information technology resources

Contact Person: Kris Estes, IT Director

Anticipated completion date: March 31, 2017

Corrective Action: Concur. The County will continue to improve disaster recovery plan, backup policies and procedures and processes to help ensure that IT systems and data necessary to conduct daily operations in the event of a disaster, system or equipment failure, or other system interruption, can be recovered and restored.

2015-07

The County should follow its policies and procedures over payroll processing

Contact Persons: Heidi Derryberry, Accounting Manager, Finance Department; Bonny Lynn, Finance Director, Finance Department

Anticipated completion date: June 30, 2016

Corrective Action: Concur. To help ensure employees are paid only for the hours they worked and payroll expenditures are accurately reported in the County's financial statements, the County policies and procedures over payroll processing will include the following steps:

- Completing the implementation of an electronic, centralized time and attendance system by June 30, 2016.

- Implementation of the *Automated Time and Attendance (1310-001) Financial Procedure* effective June 16, 2015.

- Finance Department (Payroll) review of all electronic timesheets to verify employee and supervisor level approvals are complete before the pay period is closed in the electronic time and attendance system.

Integrity ★ Accountability ★ Making a Difference ★

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

State of Arizona
Office of the Auditor General