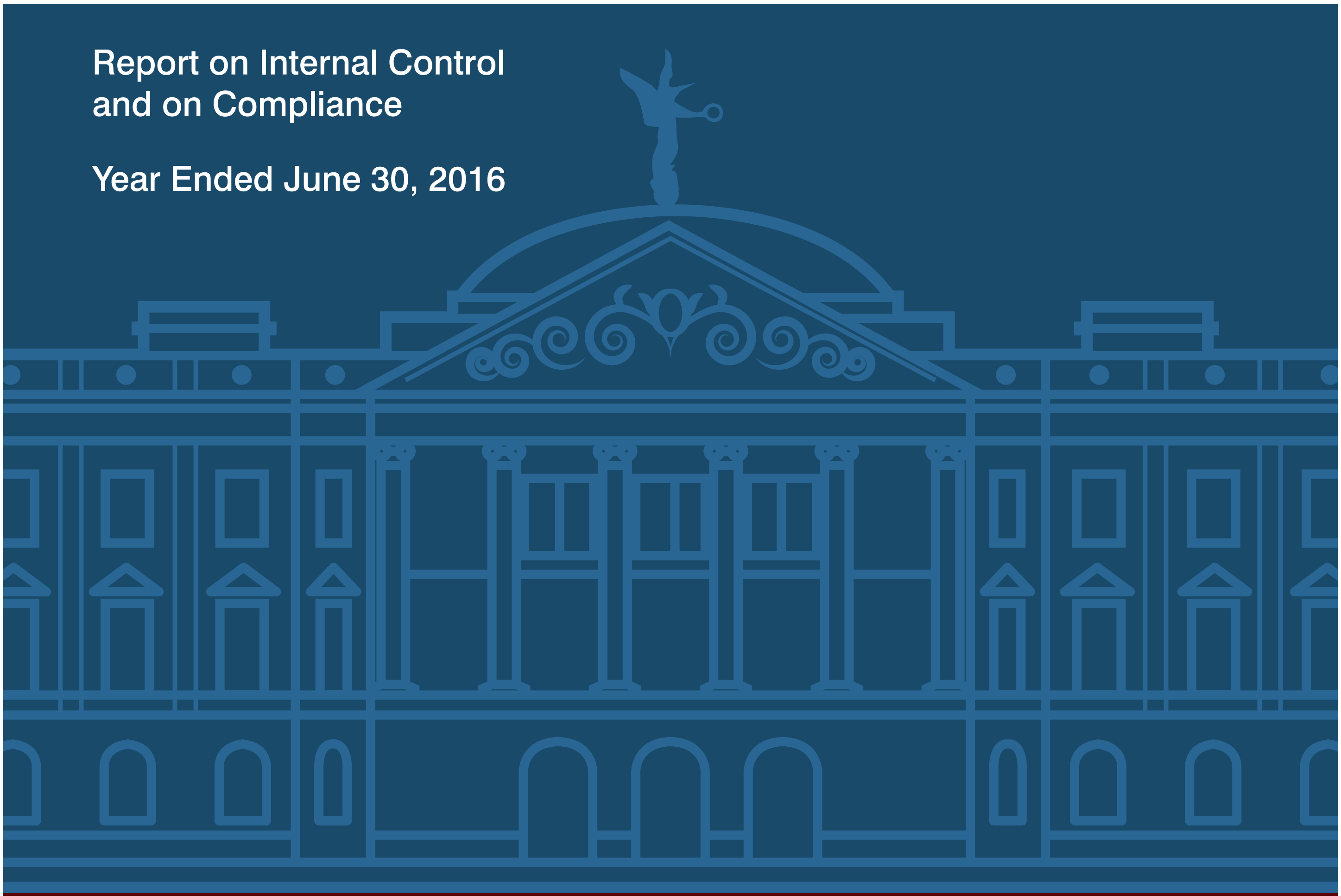
Coconino County

Report on Internal Control and on Compliance

Year Ended June 30, 2016



A Report to the Arizona Legislature

Debra K. Davenport
Auditor General

ARIZONA
Auditor General
Making a Positive Difference

ARIZONA
Auditor General
Making a Positive Difference

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 and special reviews of school districts, state agencies, and the programs they administer.

The Joint Legislative Audit Committee

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

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
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, 2016, 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 22, 2016.

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 2016-01 through 2016-06 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 deficiency described in the accompanying Schedule of Findings and Recommendations as item 2016-07 to be a significant deficiency.

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 response to findings

Coconino 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.

Jay Zsorey, CPA
Financial Audit Director

December 22, 2016

SCHEDULE OF FINDINGS AND RECOMMENDATIONS

Financial statement findings

2016-01

The County should properly report pension plan contributions

Criteria—The County should follow U.S. generally accepted accounting principles (GAAP) and its own policies and procedures when compiling its annual financial report that includes its financial statements, note disclosures, and required supplementary information. Specifically, Governmental Accounting Standards Board (GASB) Statement No. 68 requires that employer contributions made subsequent to the measurement date of the net pension liability and before the end of the employer's reporting period be reported as a deferred outflow of resources related to pensions.

Condition and context—The County made contributions to the Public Safety Personnel Retirement Plan during fiscal year 2016 that exceeded the statutorily required amount by $10 million. However, the County did not properly report the excess contributions in its financial statements, note disclosures, and required supplementary information. As a result, the County:

- Understated deferred outflows of resources related to pensions and overstated expenses by $10 million in the government-wide financial statements.
- Misclassified General Fund expenditures by $10 million in the governmental fund financial statements.
- Did not properly disclose the excess contributions in the notes to the financial statements and required supplementary information.

Effect—The County's financial statements, related note disclosures, and required supplementary information were not initially prepared in accordance with GAAP. The County made the recommended audit adjustments to the financial statements, related note disclosures, and required supplementary information for these errors, which resulted in an increase to unrestricted net position of $10 million in the government-wide financial statements.

Cause—The County was not aware of the requirements for reporting excess pension contributions.

Recommendation—The County should follow GAAP and its established policies and procedures when reporting pension plan contributions in its financial statements, note disclosures, and required supplementary information.

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

2016-02

The County should separate the responsibilities for managing and operating its information technology resources used for financial reporting

Criteria—Separating responsibilities for managing and operating the County's information technology (IT) resources used for financial reporting, which includes its financial system, system infrastructure, and financial data, helps reduce the risk of error, misuse, or fraud. Accordingly, no one individual should have full control of the County's IT resources used for financial reporting.

Condition and context—One individual is responsible for managing and operating the County's financial system. Specifically, this individual operates the infrastructure, makes all operating system and application software modifications, grants user access to the system, and manages the system's database.

Effect—Not separating incompatible responsibilities increases the possibility that errors and improper activities would not be prevented or detected. In addition, the County risks the ability to fully continue financial operations if the individual is not available.

Cause—The County's financial system has been in place for many years, and one individual has been assigned the responsibilities of managing these resources.

Recommendation—To help reduce the risk of error, misuse, or fraud, the County should separate the responsibilities for managing and operating its financial system's infrastructure and software from the responsibilities of managing the system's data and granting user access to the system.

The County'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 finding 2015-02.

2016-03

The County should improve its risk-assessment process to include information technology security

Criteria—The County faces risks of reporting inaccurate financial information and exposing sensitive data. An effective internal control system should include 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 report accurate financial information and protect sensitive data. An effective risk-assessment process provides the basis for developing appropriate risk responses and should include defining objectives to better identify risks and define risk tolerances, and identifying, analyzing, and responding to identified risks.

Condition and context—The County's annual risk-assessment process did not include a county-wide information technology (IT) security risk assessment over the County's IT resources, which include its systems, network, infrastructure, and data. Also, the County did not identify and classify sensitive information. Further, the County did not evaluate the impact disasters or other system interruptions could have on its critical IT resources.

Effect—There is an increased risk that the County's administration and IT management may not effectively identify, analyze, and respond to risks that may impact its IT resources.

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

Recommendations—To help ensure the County has effective policies and procedures to identify, analyze, and respond to risks that may impact its IT resources, the County needs to implement a county-wide IT risk-assessment process. The information below provides guidance and best practices to help the County achieve this objective.

- **Conduct an IT security risk-assessment process at least annually—**The risk-assessment process should include the identification of risk scenarios, including the scenarios' likelihood and magnitude; documentation and dissemination of results; review by appropriate personnel; and prioritization of risks identified for remediation. An IT risk assessment could also incorporate any unremediated threats identified as part of an entity's security vulnerability scans.
- **Identify, classify, inventory, and protect sensitive financial information—**Security measures should be developed to identify, classify, and inventory sensitive information and protect it, such as implementing controls to prevent unauthorized access to that information. Policies and procedures should include the security categories into which information should be classified, as well as any state statutes and federal regulations that could apply, and require disclosure to affected parties if sensitive information covered by state statutes or federal regulations is compromised.
- **Evaluate the impact disasters or other system interruptions could have on critical IT resources—**The evaluation should identify key business processes and prioritize the resumption of these functions within time frames acceptable to the entity in the event of contingency plan activation. The results of the evaluation should be considered when developing its disaster recovery plan.

The County'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 2015-05 and 2015-06.

2016-04

The County should improve access controls over its information technology resources

Criteria—Logical and physical access controls help to protect the County's information technology (IT) resources, which include its systems, network, infrastructure, and data, from unauthorized or inappropriate access or use, manipulation, damage, or loss. Logical access controls also help to ensure that authenticated users access only what they are authorized to. Therefore, 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 or consistently implement its policies and procedures to help prevent or detect unauthorized or inappropriate access to its IT resources.

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

Cause—The County developed policies and procedures during the fiscal year for granting and reviewing access to its network and systems but had not fully implemented or reviewed them to ensure they were in-line with current IT standards and best practices.

Recommendations—To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the County needs to implement effective logical and physical access controls policies and procedures over its IT resources. The information below provides guidance and best practices to help the County achieve this objective.

- **Review contractor and other nonentity account access—**A periodic review should be performed on contractor and other nonentity accounts with access to an entity's IT resources to help ensure their access remains necessary and appropriate.
- **Review user access—**A periodic, comprehensive review should be performed of all existing employee accounts to help ensure that network and system access granted is needed and compatible with job responsibilities.
- **Review and monitor key activity of users—**Key activities of users and those with elevated access should be reviewed for propriety.
- **Improve network and system password policies—**Network and system password policies should be improved and ensure they address all accounts.
- **Disable unused infrastructure—**Ethernet ports in publicly accessible areas should be disabled.
- **Implement IT standards and best practices**—IT policies and procedures over access controls should be reviewed against current IT standards and best practices, updated where needed, and implemented, as appropriate.

The County'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 finding 2015-03.

2016-05

The County should improve its configuration management processes over its information technology resources

Criteria—A well-defined configuration management process, including a change management process, is needed to ensure that the County's information technology (IT) resources, which include its systems, network, infrastructure, and data, are configured securely and that changes to these IT resources do not adversely affect security or operations. IT resources are typically constantly changing in response to new, enhanced, corrected, or updated hardware and software capabilities and new security threats. The County should have effective written configuration management internal control policies and procedures to track and document changes made to its IT resources.

Condition and context—The County did not have policies and procedures for managing changes to its financial system's IT resources, did not document all change processes for its other IT resources, and did not ensure all IT resources were configured securely.

Effect—There is an increased risk that the County's IT resources may not be configured appropriately and securely and that changes to those 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 system's IT resources because it does not typically perform changes to those resources. Additionally, for its other IT resources, the County had not reviewed its change management process to ensure it was in-line with current IT standards and best practices.

Recommendations—To help prevent and detect unauthorized, inappropriate, and unintended changes to its financial system's IT resources, the County needs to develop and implement policies and procedures over its configuration management. The information below provides guidance and best practices to help the County achieve this objective.

- **Establish and follow change management processes—**For changes to IT resources, a change management process should be established for each type of change, including emergency changes and other changes that might not follow the normal change management process. Further, all changes should follow the applicable change management process and should be appropriately documented.
- **Review proposed changes—**Proposed changes to IT resources should be reviewed for appropriateness and justification, including consideration of the change's security impact.
- **Document changes—**Changes made to IT resources should be logged and documented and a record should be retained of all change details, including a description of the change, the departments and system impacted, the individual responsible for making the change, test procedures performed and the test results, security impact analysis results, change approvals at each appropriate phase of the change management process, and a post-change review.
- **Roll back changes—**Rollback procedures should be established that include documentation necessary to back out changes that negatively impact IT resources.
- **Test—**Changes should be tested prior to implementation, including performing a security impact analysis of the change.
- **Separate responsibilities for the change management process—**Responsibilities for developing and implementing changes to IT resources should be separated from the responsibilities of authorizing, reviewing, testing, and approving changes for implementation or, if impractical, performing a post-implementation review of the change to confirm the change followed the change management process and was implemented as approved.
- **Configure IT resources appropriately and securely—**The functionality of IT resources should be limited to ensure it is performing only essential services and maintaining appropriate and secure configurations for all systems.

Further, to help prevent and detect unauthorized, inappropriate, and unintended changes to its other IT resources, the County needs to update its policies and procedures over its configuration management processes. The information below provides guidance and best practices to help the County achieve this objective.

- **Document changes—**Changes made to IT resources should be logged and documented and a record should be retained of all change details, including a description of the change, the departments and system impacted, the individual responsible for making the change, test procedures performed and the test results, security impact analysis results, change approvals at each appropriate phase of the change management process, and a post-change review.

- **Configure IT resources appropriately and securely—**The functionality of IT resources should be limited to ensure it is performing only essential services and maintaining appropriate and secure configurations for all systems.
- **Implement IT standards and best practices**—IT policies and procedures over configuration management controls should be reviewed against current IT standards and best practices, updated where needed, and implemented, as appropriate.

The County'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 finding 2015-04.

2016-06

The County should improve security over its information technology resources

Criteria—The selection and implementation of security controls for the County's information technology (IT) resources, which include its systems, network, infrastructure, and data, are important as they reduce the risks that arise from the loss of confidentiality, integrity, or availability of information that could adversely impact the County's operations or assets. Therefore, the County should implement internal control policies and procedures for an effective IT security process that include practices to help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources.

Condition and context—The County did not have sufficient written IT security policies and procedures over its IT resources.

Effect—There is an increased risk that the County may not prevent or detect the loss of confidentiality, integrity, or availability of systems and data.

Cause—The County developed policies and procedures during the fiscal year for securing its IT resources but had not fully implemented or reviewed them to ensure they were in-line with current IT standards and best practices.

Recommendations—To help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources, the County needs to further develop its policies and procedures over IT security. The information below provides guidance and best practices to help the County achieve this objective.

- **Perform proactive logging and log monitoring**—Key user and system activity should be logged, particularly for users with administrative access privileges and remote access, along with other activities that could result in potential security incidents such as unauthorized or inappropriate access. An entity 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. Finally, activity logs should be maintained where users with administrative access privileges cannot alter them.

- **Prepare and implement an incident response plan**—An incident response plan should be developed, tested, and implemented for an entity's IT resources, and staff responsible for the plan should be trained. The plan should 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. Security incidents should be reported to incident response personnel so they can be tracked and documented. Policies and procedures should also follow regulatory and statutory requirements, provide a mechanism for assisting users in handling and reporting security incidents, and making disclosures to affected individuals and appropriate authorities if an incident occurs.
- **Provide training on IT security risks**—A plan should be developed to provide continuous training on IT security risks, including 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 employees generate. Security awareness training should be provided to new employees and on an ongoing basis.
- **Perform IT vulnerability scans**—A formal process should be developed for vulnerability scans that includes performing vulnerability scans of its IT resources 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, measuring the impact of identified vulnerabilities, and approving privileged access while scanning systems containing highly sensitive data. In addition, vulnerability scan reports and results should be analyzed and legitimate vulnerabilities remediated as appropriate, and information obtained from the vulnerability-scanning process should be shared with other departments of the entity to help eliminate similar vulnerabilities.
- **Apply patches**—Patches to IT resources should be evaluated, tested, and applied in a timely manner once the vendor makes them available.
- **Secure unsupported software—**Establish a strategy for assessing and securing any software that the manufacturer no longer updates and supports.
- **Protect sensitive or restricted data—**Restrict access to media containing data the entity, federal regulation, or state statute identifies as sensitive or restricted. Such media should be appropriately marked indicating the distribution limitations and handling criteria for data included on the media. In addition, media should be physically controlled and secured until it can be destroyed or sanitized using sanitization mechanisms with the strength and integrity consistent with the data's security classification.
- **Implement IT standards and best practices—**IT policies and procedures should be reviewed against current IT standards and best practices, updated where needed, and implemented entity-wide, as appropriate. Further, staff should be trained on IT policies and procedures.

The County'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 finding 2015-05.

2016-07

The County should improve its contingency planning procedures for its information technology resources

Criteria—It is critical that the County have contingency planning 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. Contingency planning procedures include having a comprehensive, up-to-date contingency plan; taking steps to facilitate activation of the plan; and having system and data backup policies and procedures.

Condition and context—The County did not have a written contingency plan for its financial system, and its draft contingency plan for its other systems lacked certain key elements related to restoring operations in the event of a disaster or other system interruption of its IT resources. Also, although the County was performing system and data backups, it did not have documented policies and procedures for performing the backups or testing them to ensure they were operational and could be used to restore its IT resources.

Effect—The County risks not being able to provide for the continuity of operations, recover vital IT systems 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 and data recovery.

Cause—The County drafted a comprehensive disaster recovery plan; however, it was unfinished at June 30, 2016, and did not address recovery of its financial system.

Recommendations—To help ensure county operations continue in the event of a disaster, system or equipment failure, or other interruption, the County needs to further develop its contingency planning procedures. The information below provides guidance and best practices to help the County achieve this objective.

- **Update the contingency plan and ensure it includes all required elements to restore operations—** Contingency plans should be updated at least annually for all critical information or when changes are made to IT resources, and updates to the plan should be communicated to key personnel. The plan should include essential business functions and associated contingency requirements, including recovery objectives and restoration priorities and metrics as determined in the entity's business-impact analysis; contingency roles and 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 contingency 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.
- **Move critical operations to a separate alternative site—**Policies and procedures should be developed and documented for migrating critical IT operations to a separate alternative site for essential business functions, including putting contracts in place or equipping the alternative site to resume essential business functions, if necessary. The alternative site's information security safeguards should be equivalent to the primary site.

- **Test the contingency plan—**A process should be developed and documented to perform regularly scheduled tests of the contingency plan and document the tests performed and results. This process should include updating and testing the contingency plan at least annually or as changes necessitate, and coordinating testing with other plans of the entity such as its continuity of operations, 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. The test results should be used to update or change the plan.
- **Train staff responsible for implementing the contingency plan—**An ongoing training schedule should be developed for staff responsible for implementing the plan that is specific to each user's assigned role and responsibilities.
- **Backup systems and data—**Establish and document policies and procedures for testing IT system software and data backups to help ensure they could be recovered if needed. Policies and procedures should require system software and 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 stored at an alternative site or in a fire-rated container.

The County'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 finding 2015-06.

COUNTY RESPONSE

COCONINO
COUNTY ARIZONA
FINANCE

Bonny Lynn
CFO/Director

Megan Cunningham
Assistant Finance
Directorr

Jerri Garcia
Financial Systems
Manager

Tom Johnson
Financial Reporting
and Audit Manager

Scott Richardson
Purchasing Manager

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

March 1, 2017

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

Financial Statement Findings

2016-01

The County should properly report pension plan contributions

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

Completion date: December 22, 2016

Corrective Action: Concur. The County has reviewed the appropriate GAAP and its own policies and procedures related to reporting pension plan contributions in its financial statements, note disclosures, and required supplementary information and has made recommended audit adjustments to the financial statements, related note disclosures, and required supplementary information.

2016-02

The County should separate the responsibilities for managing and operating its information technology resources used for financial reporting

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

Anticipated completion date: June 30, 2018

Corrective Action: Concur. The County's current financial system does not have the capability of separating the responsibilities for managing and operating the financial system infrastructure and software from the responsibilities of managing the system data and granting user access to the system. The County will be implementing a new ERP system beginning in June 2017 that will have this capability.

In order to ensure continuity of its daily operations, the County began training a Senior Accountant in the Finance Department in April 2016 to perform duties related to managing and operating its financial accounting system.

2016-03

The County should improve its risk-assessment process to include information technology security

Contact Person: Kris Estes, IT Director

Anticipated completion date: June 30, 2018

Corrective Action: Concur. To ensure adequate policies and procedures to identify, analyze, and respond to risks that may impact IT resources, the County will develop a county-wide IT risk assessment process that incorporates NIST best practices.

2016-04

The County should improve access controls over its information technology resources

Contact Person: Kris Estes, IT Director

Anticipated completion date: June 30, 2018

Corrective Action: Concur. To help prevent and detect unauthorized access or use, manipulation, damage, or loss to IT resources, the County will develop and implement effective logical and physical access policies and procedures over its IT resources.

2016-05

The County should improve its configuration management processes over its information technology resources

Contact Person: Kris Estes, IT Director

Anticipated completion date: June 30, 2018

Corrective Action: Concur. To help prevent and detect unauthorized access or use, manipulation, damage, or loss to IT resources, the County will develop and implement effective configuration management policies and procedures over its IT resources.

2016-06

The County should improve security over its information technology resources

Contact Person: Kris Estes, IT Director

Anticipated completion date: June 30, 2018

Corrective Action: Concur. Policies and procedures are currently being drafted by the County's IT Department to improve security over its information technology resources.

2016-07

The County should improve its contingency planning procedures for its information technology resources

Contact Persons: Kris Estes, IT Director

Anticipated completion date: June 30, 2018

Corrective Action: Concur. To help ensure its operations continue in the event of a disaster, system or equipment failure, or other interruption, the County will further develop its contingency planning procedures.

ARIZONA
Auditor General
Making a Positive Difference