Navajo County

Report on Internal Control and on Compliance

Year Ended June 30, 2017

A Report to the Arizona Legislature

Debra K. Davenport
Auditor General

ARIZONA
AuditorGeneral
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

Representative **Anthony Kern**, Chair
Representative **John Allen**
Representative **Rusty Bowers**
Representative **Rebecca Rios**
Representative **Athena Salman**
Representative **J.D. Mesnard** (ex officio)

Senator **Bob Worsley**, Vice Chair
Senator **Sean Bowie**
Senator **Judy Burges**
Senator **Lupe Contreras**
Senator **John Kavanagh**
Senator **Steve Yarbrough** (ex officio)

Audit Staff

Jay Zsorey, Director
Kathleen Wood, Manager and Contact Person

Contact Information

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

(602) 553-0333

www.azauditor.gov

TABLE OF CONTENTS

Report issued separately

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
Navajo 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 Navajo County as of and for the year ended June 30, 2017, 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 18, 2017.

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 have not been 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 2017-01, 2017-03, 2017-04, and 2017-05 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 2017-02, 2017-06, and 2017-07 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*.

Navajo County response to findings

Navajo 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 18, 2017

SCHEDULE OF FINDINGS AND RECOMMENDATIONS

Financial statement findings

2017-01

The County should improve controls over year-end journal entries

Criteria—The County should have effective internal control policies and procedures to help ensure that year-end adjusting journal entries are recorded in the correct accounting period in accordance with U.S. generally accepted accounting principles (GAAP).

Condition and context—The County reported over $6 million for amounts due from other governments, but did not always have adequate internal control policies and procedures in place for preparing and reviewing year-end adjusting journal entries to help ensure that these balances were correctly recorded. Specifically, the County incorrectly accrued $546,000 in revenues that were due from other governments that were either already recorded and collected for the year or that were not earned until the subsequent fiscal year. As a result, the amounts the County initially reported for the Public Health District Fund's revenues due from other governments, and deferred inflows of resources for unavailable revenue related to intergovernmental revenue and related note disclosures were overstated.

Effect—The County's initial financial statements and note disclosures related to the Public Health District Fund were not accurate. The County made the necessary adjustments to correct these errors.

Cause—The County relied on information compiled by its Public Health District and did not follow its policies and procedures for performing a detailed review of all data and schedules used in the adjusting journal entries' preparation process to ensure that they were accurate, complete, and in accordance with GAAP.

Recommendations—To help ensure that the County's financial statements are accurate and prepared in accordance with GAAP, the County should follow its existing policies and procedures for preparing year-end adjusting journal entries, which include a detailed review of all data and schedules used in the adjusting journal entry preparation process.

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 2016-01.

2017-02

The County should improve controls over approving employees' time accounting records

Criteria—The County should maintain effective internal control policies and procedures to prepare, review, and approve documentation to support its payroll and employee-related expenses and help ensure that they are accurately recorded.

Condition and context—The County's payroll and employee-related expenses comprised over $37 million, or approximately 50 percent, of its total expenses. However, the County did not always follow its existing policies and procedures to help ensure that it prepared, reviewed, and approved documentation to support these expenses. Specifically, for 1 of 60 of employees tested, the County did not have a time sheet as required by county policy. In addition, for 2 of 60 employees tested, the employees' time sheets did not have a supervisor's review and approval, as required by county policy. Finally, for 2 of 60 employees tested, the County did not have documentation supporting the employee's pay rate changes as required by county policy.

Effect—The County risks paying employees for unauthorized charges, which also could potentially result in misstating the financial statements.

Cause—The County did not always follow its existing policies and procedures for processing payroll and employee-related expenses.

Recommendations—To help ensure that the County pays employees only for authorized charges and accurately processes and records payroll and employee-related expenses, the County should follow its existing policies and procedures requiring the preparation, review, and approval of documentation to support employees' time worked and changes to the employee records, such as pay rate changes.

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

2017-03

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.

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 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 risk-assessment process at least annually—**A 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 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.

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 2016-03.

2017-04

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 in place over its IT resources. The County had some IT security processes in place, but did not have written policies and procedures for several areas related to IT security and its policies and procedures lacked critical elements.

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 was unaware that its policies and procedures lacked critical elements related to its IT security and had not evaluated them against 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 IT security policies and procedures. The County should review these policies and procedures against current IT standards and best practices, update them where needed, and implement them county-wide, as appropriate. Further, the County should train staff on the policies and procedures. 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 and monitored, 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 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 make disclosures to affected individuals and appropriate authorities when an incident occurs.
- **Secure unsupported software—**Establish a strategy for assessing and securing any software that the manufacturer no longer updates and supports.
- **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 and existing employees on an ongoing basis.
- **Perform IT vulnerability scans—**A formal process should be developed for vulnerability scans that includes performing vulnerability scans of 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.
- **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 information's security classification.

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 2016-04.

2017-05

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 had not yet fully developed 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 was in the process of developing policies and procedures for granting and reviewing access to its IT resources, and had not fully implemented them and reviewed them against 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 develop and implement effective logical and physical access policies and procedures over its IT resources. The County should review these policies and procedures against current IT standards and best practices and implement them county-wide, as appropriate. Further, the County should train staff on the policies and procedures. The information below provides guidance and best practices to help the County achieve this objective.

- **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.
- **Remove terminated employees' access to its IT resources—**Employees' network and system access should immediately be removed upon their terminations.
- **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 all shared accounts—**Shared network access accounts should be reviewed and eliminated or minimized when possible.
- **Manage shared accounts—**Shared accounts should be used only when appropriate and in accordance with an established policy authorizing the use of shared accounts. In addition, account credentials should be reissued on shared accounts when a group member leaves.
- **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.
- **Manage employee-owned and entity-owned electronic devices connecting to the network—**The use of employee-owned and entity-owned electronic devices connecting to the network should be managed, including specifying configuration requirements and the data appropriate to access; inventorying devices; establishing controls to support wiping data; requiring security features, such as passwords, antivirus controls, file encryption, and software updates; and restricting the running of unauthorized software applications while connected to the network.
- **Manage remote access—**Security controls should be utilized for all remote access. These controls should include appropriate configuration of security settings such as configuration/connections requirements and the use of encryption to protect the confidentiality and integrity of remote sessions.
- **Review data center access**—A periodic review of physical access granted to the data center should be performed to ensure that it continues to be needed.

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 2016-05.

2017-06

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 has written policies and procedures for managing changes to its IT resources; however, the policies and procedures lacked critical elements to help ensure that change approvals were properly documented at each stage in the change process and that all changes to IT resources followed the established change process. Also, the County did not have policies and procedures to help ensure that 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 of reviews and approvals prior to being applied.

Cause—The County modeled its policies and procedures for making changes to its IT resources on another entity's policies and procedures. The County was unaware that its implementation of those policies and procedures lacked critical elements. Further, the County did not evaluate its policies and procedures against current IT standards and best practices.

Recommendations—To help prevent and detect unauthorized, inappropriate, and unintended changes to its IT resources, the County needs to further develop its configuration management policies and procedures. In addition, the County needs to review these policies and procedures against current IT standards and best practices, update them where needed, and implement them county-wide, as appropriate. Further, the County should train staff on the policies and procedures. 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 change approvals at each appropriate phase of the change management process, and a post-change review.
- **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, and maintain configuration settings—** Configure IT resources appropriately and securely, which includes limiting the functionality to ensure only essential services are performed, and maintain configuration settings for all systems.
- **Manage software installed on employee computer workstations—**For software installed on employee computer workstations, policies and procedures should be developed to address what software is appropriate and the process for requesting, approving, installing, monitoring, and removing software on employee computer workstations.

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 2016-06.

2017-07

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's contingency planning policies and procedures lacked certain key elements related to testing and restoring operations in the event of a disaster or other system interruption of its IT resources. Additionally, although the County was performing system and data backups, it did not have documented policies and procedures for securing and 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 had a contingency plan and some contingency planning processes in place. However, the County's contingency plan and contingency planning policies and procedures lacked certain key elements and had not been reviewed against current IT standards and best practices.

Recommendations—To help ensure 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 County should review its contingency planning procedures against current IT standards and best practices, update them where needed, and implement them county-wide, as appropriate. Further, the County should train staff on the policies and 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 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.
- **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.
- **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. In addition, 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. Backup 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 2016-07.

COUNTY RESPONSE

NAVAJO COUNTY

Administration

Bryan Layton	Glenn Kephart	Paige Peterson
Assistant County Manager	County Manager	Finance Director

We are Navajo County

February 9, 2018

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* and by the audit requirements of Title 2 U.S. Code of Federal Regulations Part 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*. Specifically, for each finding we are providing you with our responsible officials' views, the names of the contact people responsible for corrective action, the corrective action planned, and the anticipated completion date.

Sincerely,

Paige M. Peterson
Finance Director

Navajo County
Corrective Action Plan
Year Ended June 30, 2017

Financial Statement Findings

2017-01
The County should improve controls over year-end journal entries

Contact: Paige Peterson, Finance Director
Anticipated Completion Date: June 30, 2018

Corrective Action Plan: Concur. To help ensure that the County's financial statements are accurate and prepared in accordance with Generally Accepted Accounting Principles, we will follow our existing policies and procedures for preparing year-end journal entries which will include a detail review of the data and schedules used in the adjusting journal entry preparation.

2017-02
The County should improve controls over approving employees' time accounting records

Contact: Paige Peterson, Finance Director
Anticipated Completion Date: On-going

Corrective Action Plan: Concur. To help ensure the County pays employees for only authorized charges and accurately processes and records payroll records and expenses, we will follow our existing policies and procedures that require the preparation, review and approval of documentation to support employees' time worked and changes to the employee's records.

2017-03
The County should improve its risk-assessment process to include information technology security

Contact: Ken Dewitt, IT Director
Anticipated Completion Date: June 30, 2018

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

2017-04
The County should improve security over its information technology resources

Contact person: Ken Dewitt, IT Director
Anticipated Completion Date: June 30, 2018

Corrective Action Plan: Concur. To help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to our IT resources, we will further develop policies and procedures over IT security.

2017-05
The County should improve access controls over its information technology resources

Contact: Ken Dewitt, IT Director
Anticipated Completion Date: June 30, 2018

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

2017-06
The County should improve its configuration management processes over its information technology resources

Contact: Ken Dewitt, IT Director
Anticipated Completion Date: June 30, 2018

Corrective Action Plan: Concur. To help prevent and detect unauthorized, inappropriate, and unintended changes to its IT resources, we will improve our policies and procedures over our configuration management process.

2017-07
The County should improve its contingency planning procedures for its information technology resources

Contact: Ken Dewitt, IT Director
Anticipated Completion Date: June 30, 2018

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

ARIZONA
Auditor General
Making a Positive Difference