A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Report on Internal Control and Compliance

Navajo County

Year Ended June 30, 2014

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

Debra K. Davenport
Auditor General

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

The Auditor General's reports are available at:

www.azauditor.gov

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

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

Navajo County
Report on Internal Control and Compliance
Year Ended June 30, 2014

Table of Contents

	Page
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*	1
Schedule of Findings and Recommendations	3
County Response	8

Report Issued Separately

Comprehensive Annual Financial Report

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

Independent Auditors' Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of Basic Financial Statements Performed in Accordance with *Government Auditing Standards*

Members of the Arizona State Legislature

The Board of Supervisors of
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, 2014, 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 17, 2014.

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 2014-01 and 2014-02 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 2014-03 and 2014-04 to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the County's basic financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests 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 on pages 8 through 10. The County's responses were not subjected to the auditing procedures applied in the audit of the basic financial statements, and accordingly, we express no opinion on them.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the County's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the County's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Jay Zsorey, CPA
Financial Audit Director

December 17, 2014

Navajo County
Schedule of Findings and Recommendations
Year Ended June 30, 2014

Financial Statement Findings

2014-01

The County needs to improve security over information technology systems

Criteria: To effectively maintain and secure financial and sensitive information on the County's information technology (IT) systems, the County should establish internal control policies and procedures that include a security awareness program and practices to help prevent, detect, and respond to instances of unauthorized access or use, manipulation, damage, or loss of its IT systems, including its network, IT infrastructure, system software, and system information and data.

Condition and context: The County worked with security consultants in August 2010 to conduct an IT vulnerability assessment of its IT systems. However, the County needs to continue its remediation efforts and establish a continual process to look for and remediate vulnerabilities in its IT systems. In addition, the County needs to improve its IT security risk management and develop a security incident response plan. The County also needs to improve its IT security policies and procedures. Specifically, the County needs to have written guidance in several areas, increased training of IT personnel, and security controls and practices in place. Finally, the County did not have a security awareness program for its employees, nor did it have a training program to help ensure they were familiar with the County's security policies and procedures.

Effect: There is an increased risk that the County may not prevent or detect unauthorized access or use, manipulation, damage, or loss of its IT systems, including its network, IT infrastructure, system software, and system information and data.

Cause: The County has some processes in place to maintain and secure its IT systems, but is missing documented policies and procedures in a number of areas. Further, the County has a small IT department with no chief information security officer to oversee information security.

Recommendation: To help ensure that the County is able to effectively maintain and secure information and data on its IT systems, the County should complete its remediation efforts for vulnerabilities identified and establish a continual process to look for and remediate vulnerabilities in its IT systems. Further, the County needs a plan to keep its IT personnel up-to-date and trained on security controls and practices, and also provide training to all employees for the appropriate use of IT resources and security awareness. Finally, the County should ensure that its policies and procedures over securing its IT systems are documented in writing, implemented, and include:

- Developing a process for vulnerability assessments that involves performing IT security vulnerability reviews on a periodic basis, incorporating the results into a continual IT security risk management process, and responding to threats identified.
- Developing, updating, and testing an incident response plan on a continual basis. These policies and procedures should include incident response training and making disclosures to affected individuals and other regulatory requirements should an incident occur.

- Identifying, classifying, and inventorying sensitive information and developing security measures to protect it, such as implementing controls to prevent or detect information leaving the County's IT systems.
- Developing a strategy for assessing and securing any systems that the manufacturer may no longer support.
- Proactively logging and monitoring key activities for wireless activity, remote, and unauthorized access; user and system activity on the IT systems; and user access to the server room. Also, these controls should include a process for tracking and reviewing the activities of users with administrative access privileges for all critical IT systems and databases, and maintaining activity logs for the network where users with administrative access privileges cannot alter them.
- Managing employee-owned electronic devices connecting to the network. While the County had a process for remotely wiping lost or stolen devices that contain county data, it needs to more effectively manage employee-owned electronic devices. For example, inventorying devices; requiring security features, such as passwords, anti-virus controls, and software updates; and restricting the running of unauthorized software applications while on the County's network.
- Managing software installed on employee computer workstations. Policies and procedures should address what software is appropriate and the process for requesting, approving, installing, monitoring, and removing software on employee computer workstations.
- Managing the County's social media accounts.
- Implementing other security controls and practices, such as disabling unused Ethernet ports and removing rogue access points on the network. While the County had processes in place to identify these, it needs written guidance for these areas.

The County should also continue to enforce existing policies and procedures, such as requiring employees to sign user agreements acknowledging the appropriate use of IT resources and maintain the agreements on file.

2014-02

The County should improve access controls for its IT systems

Criteria: The County should have effective internal control policies and procedures over access to its IT systems to help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT systems, including its network, IT infrastructure, system software, and system information and data.

Condition and context: The County needs to improve policies and procedures for granting, monitoring, and removing logical and physical access to its IT systems. Specifically, the County did not have written guidance for this area. In addition, the County did not periodically monitor and review logical and physical access as well as user activity for its IT systems. Further, the County needs to employ other controls and measures to improve its access policies and procedures. Auditors performed limited tests of user access for the network and some IT systems and noted several instances of potentially inappropriate or excessive user access that the County should review.

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 systems and information and data.

Cause: Various departments operate the County's primary IT systems. Further, the County has a small IT department with no chief information security officer. The County has some processes in place, but needs to continue its efforts to strengthen access controls and oversight over IT systems on a county-wide basis.

Recommendation: To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT systems and information and data, the County should continue its efforts to establish written policies and procedures for granting, monitoring, and removing logical and physical access for its IT systems that include the following:

- Documenting all requests and approvals of user access granted to its IT systems. Also, defining access roles that are based on the employees' job responsibilities when setting up access to help prevent incompatible user access assignments. Further, using defined user access roles for each IT system so that consistent application and approval of the user access roles can be performed.
- Removing users' access to IT systems, including the network, immediately upon termination of employment.
- Performing a periodic, comprehensive review of all existing user accounts for its network and IT systems to help ensure that access granted is appropriate and compatible with job responsibilities. Also, investigating user accounts that auditors identified as potentially having inappropriate or excessive access privileges and removing them as appropriate.
- Logging and periodically monitoring users' access and activities on the IT systems and network, especially users with administrative-level access and elevated access privileges.
- Strengthening password and log-in controls.
- Restricting physical access to the data center and periodically reviewing access granted to the data center to ensure that it is needed and compatible with employees' job responsibilities.
- Protecting network closets from unauthorized access and physical damage by securing them and employing fire suppression and other physical safeguards.

This finding is similar to a prior-year finding.

2014-03

The County should improve its IT change management processes

Criteria: The County should have adequate change management internal control policies and procedures to track and document changes made to its IT systems, including its network, IT infrastructure, system software, and databases. Such policies and procedures will help prevent and detect unauthorized, inappropriate, or unintended changes.

Condition and context: The County did not have written policies and procedures for managing changes to its IT systems, including its network, IT infrastructure, system software, and databases. While the County had a process for making changes to some of its IT systems and infrastructure, it needs to expand its existing processes to address changes made to all of its critical IT systems and infrastructure. Further, the County's processes did not address documenting all changes, including test results, approvals, and

procedures to revert back to the state before the change in the event the change does not work as intended. Also, the County's tests included live data instead of dummy data. In addition, the County did not separate the responsibilities of employees making changes and implementing them. For example, auditors found that certain users had the ability to approve software patches and system and hardware configurations and also implement them without an independent review of the changes. Finally, the County did not have a process for detecting unauthorized, inappropriate, or unintended changes. For example, there was no post-change process to reconcile changes made to the change requests to help ensure that changes were authorized and worked as intended and that no changes circumvented controls.

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

Cause: Various departments operate the County's primary IT systems. Further, the County has a small IT department with some processes in place, but needs to continue its efforts to strengthen change management policies and procedures on a county-wide basis.

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

- Tracking all changes to its critical IT systems, including its network, IT infrastructure, system software, and databases.
- Logging and documenting all changes, including test results and approvals.
- Implementing rollback or fallback procedures into the change management process in the event that changes do not work as intended.
- Testing and approving all changes. This process should also include software patches and system and hardware configurations.
- Using dummy data for developing and testing changes.
- Separating the responsibilities for developing and implementing changes from the responsibilities of authorizing, reviewing, testing, and approving changes for implementation.
- Prohibiting users from making changes and bypassing the change management process.
- Developing a process for ensuring that unauthorized, inappropriate, or unintended changes are prevented or detected. This process should include a reconciliation and review of changes after implementation to the change requests to help ensure that changes have the intended impact.

2014-04

The County needs to improve its disaster recovery plan and data backup processes

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 ensure that vital IT systems and data can be recovered in the event of a disaster, system or equipment failure, or other system interruption.

Condition and context: The County had some recovery and backup processes in place, but needed to continue improving these processes to help ensure that it could efficiently recover its IT systems and data vital to its operations in the event of a disaster, system or equipment failure, or other system interruption. Specifically, the County needs to keep its disaster recovery plan up-to-date and test the plan annually and update the plan for any problems noted. While the County tested some elements of its disaster recovery plan, its process did not include performing regularly scheduled, comprehensive tests and documenting test results. Auditors performed limited procedures on the County's disaster recovery plan and found that some assumptions the County made for recovering its IT systems at the alternative recovery site did not appear reasonable. Finally, the County needs to improve its processes for securing and testing backup data to help ensure that it is protected and can be recovered.

Effect: The County is at risk of not being able to recover IT systems and data and conduct daily operations in the event of a system or equipment failure or other interruption, which could cause inaccurate or incomplete system information and data, expensive recovery efforts, and financial losses.

Cause: The County has a small IT department with some processes in place for testing elements of its disaster recovery plan. However, the County's tests and policies and procedures for this area were not comprehensive enough to keep the plan up-to-date and ensure that the County could carry out the plan in the event that it is needed.

Recommendation: The County should improve its disaster recovery plan and data backup policies and procedures to help ensure that it can recover its IT systems and data necessary to conduct daily operations in the event of a disaster, system or equipment failure, or other system interruption. Specifically, the County should:

- Ensure that its disaster recovery plan contains all critical information, such as a current listing of key personnel assigned to disaster recovery teams and emergency contact information.
- 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. 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. Test results should also be used to update or change the plan.
- Establish policies and procedures for testing backups of IT systems and data to help ensure that the County could recover them in the event that they are needed. Policies and procedures should require data backups to be protected with encryption methods.

This finding is similar to a prior-year finding.

COUNTY RESPONSE

NAVAJO COUNTY

FINANCE DEPARTMENT

James Menlove • Finance Director Mary Springer • Deputy Finance Director

"Proudly Serving, Continuously Improving"

February 10, 2015

Debbie Davenport
Auditor General
2910 North 44th Street, Suite 410
Phoenix, AZ 85018

Dear Ms. Davenport:

The accompanying Corrective Action Plan has been prepared as required by U.S. Office of Management and Budget Circular A-133. Specifically, we are providing you with the name of the contact person responsible for corrective action, the corrective action planned, and the anticipated completion date for each audit finding included in the current year's Schedule of Findings and Recommendations.

Sincerely,

W. James Menlove, CPA
Finance Director

• 928.524.4343 • Fax: 928.524.4239 • P.O. Box 668 • Holbrook, AZ 86025 •
• www.navajocountyaz.gov •

Navajo County
Corrective Action Plan
Year Ended June 30, 2014

2014-01

The County needs to improve security over information technology systems

Contact person: James Menlove, Finance Director, 928-524-4343
Anticipated Completion Date: June 30, 2015

Corrective Action Plan: 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.

2014-02

The County should improve access controls for its IT systems

Contact person: James Menlove, Finance Director, 928-524-4343
Anticipated Completion Date: June 30, 2015

Corrective Action Plan: 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.

2014-03

The County should improve its IT change management processes

Contact person: James Menlove, Finance Director, 928-524-4343
Anticipated Completion Date: June 30, 2015

Corrective Action Plan: 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.

Navajo County
Corrective Action Plan
Year Ended June 30, 2014

2014-04

The County needs to improve its disaster recovery plan and data backup processes

Contact person: James Menlove, Finance Director, 928-524-4343
Anticipated Completion Date: June 30, 2015

Corrective Action Plan: Concur. The County will continue to improve disaster recovery plan and 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.

Navajo County
Report on Internal Control and Compliance
Year Ended June 30, 2014

State of Arizona
Office of the Auditor General