A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Report on Internal Control and Compliance

Navajo County

Year Ended June 30, 2015

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

Debra K. Davenport
Auditor General

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

The Auditor General's reports are available at:

www.azauditor.gov

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

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

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

Table of Contents

Report Issued Separately

Comprehensive Annual Financial Report

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

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

Members of the Arizona State Legislature

The Board of Supervisors of
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, 2015, and the related notes to the financial statements, which collectively comprise the County's basic financial statements, and have issued our report thereon dated December 16, 2015.

Internal Control over Financial Reporting

In planning and performing our audit of the financial statements, we considered the County's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the basic financial statements, but not for the purpose of expressing an opinion on the effectiveness of the County's internal control. Accordingly, we do not express an opinion on the effectiveness of the County's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies, and therefore, material weaknesses or significant deficiencies may exist that were not identified. However, as described in the accompanying Schedule of Findings and Recommendations, we identified certain deficiencies in internal control over financial reporting that we consider to be material weaknesses and significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the County's basic financial statements will not be prevented, or detected and corrected, on a timely basis. We consider the deficiencies described in the accompanying Schedule of Findings and Recommendations as items 2015-01 and 2015-02 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 2015-03 and 2015-04 to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the County's basic financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests 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 9 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 16, 2015

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

Financial Statement Findings

2015-01

The County should improve security over its information technology resources

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

Condition and context: The County did not have established policies and procedures in place for several areas related to IT security. Specifically, the County did not:

- Develop a county-wide IT security risk assessment process.
- Have a continual process to identify vulnerabilities in its IT resources, nor did it have a plan to prioritize and remediate or mitigate identified vulnerabilities.
- Identify and categorize data by sensitivity and take appropriate action to protect sensitive information.
- Provide continual training to keep IT personnel up to date on IT security risks, controls and practices. In addition, the County did not have a security awareness program for all employees, nor did it have a training program to help ensure that they were familiar with the County's IT security policies and procedures.
- Establish a process to respond to security incidents.
- Log and monitor key user and system activity.
- Use updated software for all of its systems.
- Require appropriate security measures for employee-owned electronic devices with access to the County's network and monitor these devices' use. Specifically, while the County inventoried employee-owned devices and had procedures to remove information from them if needed, it did not have policies and procedures to guide their use, specify what information they could access, and require that they have security features in place.
- Manage the installation of software on employee computer workstations. For example, the County had no written policy or process to identify what software is appropriate, and had no process to monitor and detect unauthorized software.
- Have a policy or process for protecting digital and nondigital media.
- Restrict access to IT resources in public areas.

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 resources.

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

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

- Developing a county-wide IT security risk assessment process that is performed at least annually and includes the identification of risk scenarios that could impact the County, including the scenarios' likelihood and magnitude; documentation and dissemination of results; review by appropriate personnel; and prioritization of risks identified for remediation. Also, incorporate any threats identified as part of the County's IT security vulnerability scans into the IT security risk assessment process.
- Developing a formal process to identify vulnerabilities that includes performing IT vulnerability scans on a periodic basis and utilizing tools and techniques to automate parts of the process by using standards to reveal software flaws and improper configuration, formatting procedures to test the presence of vulnerabilities, and measuring the impact of identified vulnerabilities. In addition, the County should analyze vulnerability scan reports and results, and prioritize and remediate legitimate vulnerabilities as appropriate.
- Identifying, categorizing, and inventorying sensitive information and developing security measures to protect it, such as implementing controls to prevent unauthorized access to that information. The County's policies should include the security categories into which information should be categorized, as well as the state and federal laws and regulations that impact those security classifications.
- Developing a plan to provide continual training on IT security risks, controls, and practices for the County's IT personnel. In addition, the County should develop a security awareness training program for all employees that provides a basic understanding of information security, user actions to maintain security, and how to recognize and report potential indicators of security threats, including threats other county employees generate. Provide such training to new and existing users on an on-going basis as determined by the County.
- Establishing and documenting a process to respond to security incidents. This process should include developing and testing an incident response plan and training staff responsible for the plan. The plan should define reportable incidents and address steps on how to identify and handle incidents that include preparation, detection and analysis, containment, eradication, and recovery. The plan should also coordinate incident-handling activities with contingency-planning activities and incorporate lessons learned from ongoing incident handling into the incident response procedures. The incident response plan should be distributed to incident response personnel and updated, as necessary. Suspected incidents should be reported to incident response personnel so the County can track and document incidents. The County should also ensure that these policies and procedures follow regulatory and statutory requirements, provide a mechanism for assisting personnel in handling and reporting security incidents, and include making disclosures to affected individuals and appropriate authorities should an incident occur.
- Logging and monitoring logs of key activities on a proactive basis. Examples of key activities include remote and unauthorized access, server room access, key user and system activity and key wireless activity, including wireless access points not belonging to the County, along with other activities that could result in potential security incidents such as unauthorized access. The County should determine what events to log, configure the system to generate the logs, and decide how often to monitor the logs for indications of potential attacks or misuse of IT resources. Also, policies and procedures 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 where users with administrative access privileges cannot alter them.

- Implementing a strategy for assessing and securing any software that the manufacturer no longer updates and supports.
- Managing employee-owned electronic devices connecting to the network, including specifying the data appropriate to access; requiring security features, such as passwords, antivirus 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.
- Developing media protection policies and procedures to restrict access to media containing data the County, federal regulation, or state statute identifies as sensitive or restricted. Such policies and procedures should require that the County appropriately mark media indicating the distribution limitations and handling caveats given the data included on the media. In addition, the County should physically control and secure such media until it can destroy or sanitize it using sanitization mechanisms with the strength and integrity commensurate with the information's security classification.
- Implementing a process to disable unused Ethernet ports in public areas to help protect the County's IT resources from being used for inappropriate or illegal activities.

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

2015-02

The County should improve access controls over its information technology resources

Criteria: The County should have effective internal control policies and procedures to control access to its information technology (IT) resources, which include its systems, network, infrastructure, and data.

Condition and context: The County did not have policies and procedures for assigning, granting, removing, and reviewing logical access to its systems, network, and data, and for permitting physical access to its data center. Specifically, the County had no processes for assigning system access based on job responsibilities or reviewing user access privileges for appropriateness. Auditors noted that the County allowed terminated employees and an excessive number of current employees access to critical IT resources, with some users having administrator-level access or access that was incompatible with job responsibilities. Additionally, the County did not have adequate network password policies because passwords, including those for administrator accounts, were set to never expire, and the County's network lockout configurations and other security features were either insufficient or disabled. Finally, auditors noted that, although the County logged and reviewed who accessed the data center, it did not periodically review employees authorized to access the data center to ensure that their access remained appropriate. Also, the County did not adequately protect its data center and network closets against fire and physical damage.

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 resources, including sensitive and confidential information.

Cause: The County focused its efforts on the day-to-day operations and did not prioritize its review of IT policies and procedures for access against IT standards and best practices.

Recommendation: To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the County should develop and implement policies and procedures for assigning, granting, removing, and reviewing access that include the following:

- Performing a periodic, comprehensive review of all existing employee access accounts to ensure that network and system access granted is needed and compatible with job responsibilities.
- Removing employees' network and system access immediately upon their terminations.
- Reviewing employees' network and system access immediately when their job responsibilities change to ensure that access granted is compatible with their new job responsibilities.
- Reviewing all service and administrator access accounts to eliminate or minimize their use when possible.
- Reviewing and monitoring the activity of users with elevated access for propriety.
- Strengthening network password policies by requiring employees to change passwords on a periodic basis and by improving and enabling lockout and other security features.
- Restricting data center access to employees who need it for their job responsibilities and periodically reviewing access granted to ensure that it continues to be needed.
- Protecting the data center and network closets from unauthorized access and physical damage by securing them and employing fire suppression and other physical safeguards.

This finding is similar to prior-year finding 2014-02.

2015-03

The County should improve its information technology change management process

Criteria: The County should have adequate change management internal control policies and procedures to track and document changes made to its IT resources, which include its systems, network, infrastructure, and data.

Condition and context: The County developed written policies and procedures and a process for managing changes to its IT resources at the beginning of the year. However, the County did not follow the process it developed for making changes to operating systems, infrastructure, and network configuration. Further, the County did not ensure that (1) change documentation consistently included key elements, such as test results, approvals, and procedures to revert back to the state before the change if the change does not work as intended; (2) responsibilities of employees making changes and implementing changes were separated; and (3) vendors' implementation of software patches and other changes were reviewed, tested and approved. Finally, the County's tests included live data instead of dummy data.

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

Cause: The County modeled its policies and procedures based on another entity's, and was unaware that its implementation of those policies and procedures lacked critical elements. Further, it did not evaluate its policies and procedures against current IT standards and best practices.

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

- Reviewing its written policies and procedures and change management process against IT standards and best practices to ensure that they address all changes to critical IT resources, including patch management of software systems and changes to operating systems, infrastructure, and network configuration.
- Implementing a way of logging and controlling changes to critical IT resources to ensure that all changes follow established change management policies and procedures and are appropriately documented.
- Documenting key elements for all changes, including test results and approvals.
- Incorporating rollback procedures that back out changes that negatively impact IT resources.
- Testing and approving all changes, including software patches and system and hardware configurations.
- Testing, authorizing, and storing configuration for servers, routers, switches, and other critical IT resources.
- 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.
- Using dummy data for developing and testing changes.

This finding is similar to prior-year finding 2014-03.

2015-04

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

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

Condition and context: Auditors reviewed the County's disaster recovery plan and processes and determined that they lacked certain key elements for restoring operations. Specifically, the County did not:

- Update critical information in its disaster recovery plan, including the list of key personnel assigned to disaster recovery teams and emergency contact information.

- Perform regularly scheduled, comprehensive tests; document test results; and update the plan for any problems noted. The County performed tests in a virtual setting for restoring all its computers at its designated off-site location; however, auditors' analysis of the off-site location revealed that its capacity was not sufficient to accommodate the number of computers needed during normal operations.
- Secure and test backup data to help ensure that backup data was protected and can be recovered when needed.

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

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

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

- Ensure that its disaster recovery plan is updated for 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, comprehensive 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 securing and testing backup data on a regular basis to help ensure that they are protected and could be recovered in the event that they are needed.

This finding is similar to prior-year finding 2014-04.

COUNTY RESPONSE

NAVAJO COUNTY
FINANCE DEPARTMENT
James Menlove • Administrative Services Director
"Proudly Serving, Continuously Improving"

February 11, 2016

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
Administrative Services 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, 2015

2015-01
The County should improve security over its information technology resources

Contact: Ken Dewitt, IT Director
Anticipated Completion Date: June 30, 2016

Corrective Action Plan: Concur. To help ensure that the County is able to effectively maintain and secure IT resources the County will ensure that policies and procedures over securing IT resources are documented in writing and implemented.

2015-02
The County should improve access controls over its information technology resources

Contact person: Ken Dewitt, IT Director
Anticipated Completion Date: June 30, 2016

Corrective Action Plan: Concur. To help prevent and detect unauthorized access or use, manipulation, damage, or loss to IT resources the County will develop and implement policies and procedures for assigning, granting, removing, and reviewing access.

2015-03
The County should improve its information technology change management process

Contact person: Ken Dewitt, IT Director
Anticipated Completion Date: June 30, 2016

Corrective Action Plan: Concur. To help prevent and detect unauthorized, inappropriate, and unintended changes to IT resources the County will follow the processes developed and improve written change management policies and procedures.

2014-04
The County should improve its disaster recovery plan and data backup procedures for its information technology resources

Contact person: Ken Dewitt, IT Director
Anticipated Completion Date: June 30, 2016

Corrective Action Plan: Concur. To help ensure the continuity of the County's operations in the event of a disaster, system or equipment failure, or other system interruption the County will ensure the information technology continuity of operations policies and procedures are documented and implemented.

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

State of Arizona
Office of the Auditor General