Graham County

Single Audit Report

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

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

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

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
Graham 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 Graham 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 March 30, 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 were not identified. However, as described in the accompanying schedule of findings and questioned costs, we identified certain deficiencies in internal control over financial reporting that we consider to be a material weakness 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 deficiency described in the accompanying schedule of findings and questioned costs as item 2016-01 to be a material weakness.

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 questioned costs as items 2016-02, 2016-03, 2016-04, 2016-05, 2016-06, and 2016-07 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.*

Graham County's response to findings

Graham 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

March 30, 2017

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

Independent auditors' report on compliance for each major federal program; report on internal control over compliance; and report on schedule of expenditures of federal awards required by the Uniform Guidance

Members of the Arizona State Legislature

The Board of Supervisors
Graham County, Arizona

Report on compliance for each major federal program

We have audited Graham County's compliance with the types of compliance requirements described in the *U.S. Office of Management and Budget (OMB) Compliance Supplement* that could have a direct and material effect on each of its major federal programs for the year ended June 30, 2016. The County's major federal programs are identified in the summary of auditors' results section of the accompanying schedule of findings and questioned costs.

Management's responsibility

Management is responsible for compliance with federal statutes, regulations, and the terms and conditions of its federal awards applicable to its federal programs.

Auditors' responsibility

Our responsibility is to express an opinion on compliance for each of the County's major federal programs based on our audit of the types of compliance requirements referred to above. We conducted our audit of compliance in accordance with U.S. generally accepted auditing standards; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and 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* (Uniform Guidance). Those standards and the Uniform Guidance require that we plan and perform the audit to obtain reasonable assurance about whether noncompliance with the types of compliance requirements referred to above that could have a direct and material effect on a major federal program occurred. An audit includes examining, on a test basis, evidence about the County's compliance with those requirements and performing such other procedures as we considered necessary in the circumstances.

We believe that our audit provides a reasonable basis for our opinion on compliance for each major federal program. However, our audit does not provide a legal determination of the County's compliance.

Opinion on each major federal program

In our opinion, Graham County complied, in all material respects, with the types of compliance requirements referred to above that could have a direct and material effect on its major federal program for the year ended June 30, 2016.

Report on internal control over compliance

The County's management is responsible for establishing and maintaining effective internal control over compliance with the types of compliance requirements referred to above. In planning and performing our audit of compliance, we considered the County's internal control over compliance with the types of requirements that could have a direct and material effect on each major federal program to determine the auditing procedures that are appropriate in the circumstances for the purpose of expressing an opinion on compliance for each major federal program and to test and report on internal control over compliance in accordance with the Uniform Guidance, but not for the purpose of expressing an opinion on the effectiveness of internal control over compliance. Accordingly, we do not express an opinion on the effectiveness of the County's internal control over compliance.

A deficiency in internal control over compliance exists when the design or operation of a control over compliance does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, noncompliance with a type of compliance requirement of a federal program on a timely basis. A material weakness in internal control over compliance is a deficiency, or a combination of deficiencies, in internal control over compliance, such that there is a reasonable possibility that material noncompliance with a type of compliance requirement of a federal program will not be prevented, or detected and corrected, on a timely basis. A significant deficiency in internal control over compliance is a deficiency, or a combination of deficiencies, in internal control over compliance with a type of compliance requirement of a federal program that is less severe than a material weakness in internal control over compliance, yet important enough to merit attention by those charged with governance.

Our consideration of internal control over compliance was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over compliance that might be material weaknesses or significant deficiencies. We did not identify any deficiencies in internal control over compliance that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified.

The purpose of this report on internal control over compliance is solely to describe the scope of our testing of internal control over compliance and the results of that testing based on the requirements of the Uniform Guidance. Accordingly, this report is not suitable for any other purpose.

Report on schedule of expenditures of federal awards required by the Uniform Guidance

We have audited the financial statements of the governmental activities, each major fund, and aggregate remaining fund information of Graham 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. We issued our report thereon dated March 30, 2017, that contained unmodified opinions on those financial statements. Our audit was conducted for the purpose of forming our opinions on the financial statements that collectively comprise the County's basic financial statements. The accompanying schedule of expenditures of federal awards is presented for purposes of additional analysis as required by the Uniform Guidance and is not a required part of the basic financial statements. Such information is the responsibility of the County's management and was derived from and relates directly to the underlying accounting and other records used to prepare the basic financial statements. The information has been subjected to the

auditing procedures applied in the audit of the basic financial statements and certain additional procedures, including comparing and reconciling such information directly to the underlying accounting and other records used to prepare the basic financial statements or to the basic financial statements themselves, and other additional procedures in accordance with U.S. generally accepted auditing standards. In our opinion, the schedule of expenditures of federal awards is fairly stated in all material respects in relation to the basic financial statements as a whole.

Jay Zsorey, CPA
Financial Audit Director

March 30, 2017


ARIZONA
Auditor General
Making a Positive Difference

Summary of auditors' results

Financial statements

Type of auditors' report issued on whether the financial statements audited were prepared in accordance with generally accepted accounting principles	Unmodified
Internal control over financial reporting	
Material weakness identified?	Yes
Significant deficiencies identified?	Yes
Noncompliance material to the financial statements noted?	No

Federal awards

Internal control over major programs	
Material weakness identified?	No
Significant deficiency identified?	None reported
Type of auditors' report issued on compliance for major programs	Unmodified
Any audit findings disclosed that are required to be reported in accordance with 2 CFR 200.516(a)?	No
Identification of major programs	

CFDA number	Name of federal program or cluster
15.226	Payments in Lieu of Taxes

Dollar threshold used to distinguish between Type A and Type B programs	$750,000
Auditee qualified as low-risk auditee?	No

Other matters

Auditee's summary schedule of prior audit findings required to be reported in accordance with 2 CFR 200.511(b)?	Yes

Financial statement findings

2016-01

The County should establish procedures to accurately record and report financial information

Criteria—The County should have policies and procedures to help ensure that its annual financial report that includes its financial statements, note disclosures, and required supplementary information is accurately compiled and prepared in accordance with U.S. generally accepted accounting principles (GAAP). The County's Board of Supervisors and management depend on accurate financial statements prepared in accordance with GAAP to fulfill their oversight responsibilities and to report accurate financial information to the public and agencies from which the County receives funding.

Condition and context—The County did not accurately compile and thoroughly review its annual financial report. As a result, the County's annual financial report contained misstatements and errors that required correction. For example, deferred outflows related to pensions, pension expenses, investments held by trustee, long-term debt, and net position amounts were not accurately reported. Further, the deposits and investments, long-term debt, and pension notes contained errors or were incomplete.

Effect—Without a detailed review, the County's annual financial report could misstate amounts reported, omit important and required information, or contain other misstatements and errors. The County adjusted its financial statements, note disclosures, and required supplementary information to report the correct amounts and other required information.

Cause—The County lacked comprehensive written policies and procedures needed to accurately prepare and perform a thorough review of its annual financial report.

Recommendations—To help ensure that the County's annual financial report is accurate and prepared in accordance with GAAP, the County should develop and implement comprehensive written policies and procedures for compiling and presenting financial data within its annual financial report. The policies and procedures should include detailed instructions for compiling data from the County's accounting system and for obtaining information not readily available from the accounting system but necessary for financial statement preparation. The policies and procedures should require an employee, knowledgeable of GAAP and who did not prepare the annual financial report, to perform a detailed review of it. The reviewer should make sure that the amounts are accurate and properly supported and the annual financial report is presented in accordance with GAAP.

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 improve its policies and procedures over purchasing

Criteria—An effective purchasing system allows a county to identify the goods and services required for county operations and acquire them as economically as possible within acceptable standards of quality. Counties should have internal controls over purchasing that provide adequate authorization of and accountability for county expenditures and ensure that procurement policies are consistent with legal requirements and sound business practices.

Condition and context—The County did not have adequate policies and procedures in place to address the various purchasing requirements. Auditors tested ten purchases made through the formal purchasing process and found the following:

- The County awarded two competitive bid purchases to vendors who were not the lowest bidder, and the County did not retain documents to support vendor selection, including an explanation why it did not select the vendor with the lowest bid.
- The County awarded two sole source purchases to vendors whom it determined to be sole source providers of the goods needed; however, the County did not retain documents to support its sole source vendor determination.
- The County made one emergency purchase; however, the County did not prepare a written request documenting that an emergency condition existed and explaining the immediate purchase need, the supplier's name, the procurement's duration and estimated amount, and that the price submitted was fair and reasonable. In addition, the County did not, at the first scheduled meeting following the emergency purchase, provide to the Board of Supervisors a report concerning the emergency purchase.
- The County used a state contract for one purchase; however, the County did not perform due diligence to ensure the contract was procured through competitive procedures reasonably similar to county procedures.

Effect—The County could make potentially less advantageous purchases.

Cause—The County did not have adequate policies and procedures in place to address the various purchasing requirements.

Recommendations—The County should develop purchasing policies and procedures in sufficient detail to identify employees' responsibilities, duties, and tasks within the purchasing system. These policies and procedures should be in writing and distributed to employees involved in the purchasing process. The information below provides guidance and best practices to help the County acquire goods and services as economically as possible within acceptable standards of quality:

- Document in writing why the quote or bid selected is more advantageous to the County when it is not the lowest quote or bid.
- Document in writing why a vendor is determined to be a sole source vendor.
- Document in writing why an emergency purchase was determined to be an emergency and why the vendor chosen was selected. Also, at the first scheduled meeting following the emergency purchase, provide to the Board of Supervisors a report concerning the emergency purchase.
- Document in writing what due diligence was performed to determine purchases under state contract were procured in a similar manner to the County's purchasing procedures.

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

2016-03

The County should improve access controls over its information technology resources

Criteria—Logical and physical access controls help to protect a 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 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 has no one dedicated to ensuring policies and procedures are written and up to date.

Recommendations—To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the County needs to develop and implement effective logical access policies and procedures over its IT resources. 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 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 2015-01.

2016-04

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 IT resources to ensure changes were properly documented, authorized, reviewed and tested, and approved. Also, the County did not have policies and procedures to ensure 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 focused its efforts on the day-to-day operations and did not prioritize its IT configuration management policies and procedures.

Recommendations—To help prevent and detect unauthorized, inappropriate, and unintended changes to its 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(s) 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.

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.

2016-05

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 focused its efforts on the day-to-day operations and did not prioritize its IT risk-assessment policies and procedures.

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 2015-04.

2016-06

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 plan 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 has some processes in place but lacks a sufficiently documented contingency 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.

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.

- **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 2015-03.

2016-07

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's policies and procedures lacked critical elements related to IT security, and the County did not evaluate its policies and procedures 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 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.
- **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 2015-04.

Federal award findings and questioned costs

None reported.

COUNTY SECTION

Graham County
Schedule of expenditures of federal awards
Year ended June 30, 2016

Federal agency/CFDA number	Federal program name	Cluster title	Pass-through grantor	Pass-through grantor's numbers	Program expenditures
Department of Agriculture					
10 555	National School Lunch Program	Child Nutrition Cluster	Arizona Department of Education	None	$ 15,170
10 557	Special Supplemental Nutrition Program for Women, Infants, and Children		Arizona Department of Health Services	ADHS14-053054	193,693
10 665	Schools and Roads—Grants to States	Forest Service Schools and Roads Cluster			454,018
10 904	Watershed Protection and Flood Prevention				40,000
	Total Department of Agriculture				702,881
Department of Housing and Urban Development					
14 228	Community Development Block Grants/State's Program and Non-Entitlement Grants in Hawaii		Arizona Department of Housing	112-12, 117-14	24,115
Department of the Interior					
15 226	Payments in Lieu of Taxes				3,020,172
Department of Justice					
16 606	State Criminal Alien Assistance Program				135
16 607	Bulletproof Vest Partnership Program				7,281
16 738	Edward Byrne Memorial Justice Assistance Grant Program				17,263
16 738	Edward Byrne Memorial Justice Assistance Grant Program		Arizona Criminal Justice Commission	DC-16-024, DC-16-005	31,418
	Total 16.738				48,681
	Total Department of Justice				56,097
Department of Education					
84 010	Title I Grants to Local Educational Agencies		Arizona Department of Education	16FT1FFI-613185-01A	26,922
84 013	Title I State Agency Program for Neglected and Delinquent Children and Youth		Arizona Supreme Court	16FT1NAD-617161-46B	29,001
84 013	Title I State Agency Program for Neglected and Delinquent Children and Youth		Arizona Supreme Court/Greenlee County	16FT1NAD-617161-46B	9,727
	Total 84.013				38,728
84 027	Special Education—Grants to States	Special Education Cluster (IDEA)	Arizona Department of Education	16FESSCG-613189-55B, 16FESCBG-613185-09A	489,245
84 027	Special Education—Grants to States	Special Education Cluster (IDEA)	Arizona Supreme Court	16FESCBG-617161-09A, 16FESSCG-617161-55B, KR15-0008	33,411
84 027	Special Education—Grants to States	Special Education Cluster (IDEA)	Arizona Supreme Court/Greenlee County	16FESCBG-617161-09A, 16FESSCG-617161-55B, KR15-0009	7,439
	Total 84.027				530,095
84 173	Special Education—Preschool Grants	Special Education Cluster (IDEA)	Arizona Department of Education	16FECCBP-613185-37A	19,494
	Total Special Education Cluster (IDEA)				549,589
84 358	Rural Education				12,560
84 367	Improving Teacher Quality State Grants		Arizona Supreme Court/Greenlee County	16FT1TII-617161-03A	2,506

See accompanying notes to schedule.

Graham County
Schedule of expenditures of federal awards
Year ended June 30, 2016

Federal agency/CFDA number	Federal program name	Cluster title	Pass-through grantor	Pass-through grantor's numbers	Program expenditures
84 367	Improving Teacher Quality State Grants		Arizona Supreme Court	16FT1TII-617161-03A	11,130
	Total 84.367				13,636
	Total Department of Education				641,435
Department of Health and Human Services					
93 069	Public Health Emergency Preparedness		Arizona Department of Health Services	ADHS12-007888	175,229
93 539	PPHF Capacity Building Assistance to Strengthen Public Health Immunization Infrastructure and Performance Financed in Part by Prevention and Public Health Funds		Arizona Department of Health Services	ADHS13-041540	81,198
93 940	HIV Prevention Activities—Health Department Based		Arizona Department of Health Services	ADHS13-031211	6,748
93 991	Preventive Health and Health Services Block Grant		Arizona Department of Health Services	ADHS12-020645, ADHS15-078130	71,298
93 994	Maternal and Child Health Services Block Grant to the States		Arizona Department of Health Services	ADHS13-034537	49,906
	Total Department of Health and Human Services				384,379
Department of Homeland Security					
97 042	Emergency Management Performance Grants		Arizona Department of Emergency and Military Affairs	EMW-2015-EP-00048	39,004
97 067	Homeland Security Grant Program		Arizona Department of Emergency and Military Affairs	14-AZDOHS-HSGP-140304-01, 140308-01, 150308-01	168,151
	Total Department of Homeland Security				207,155
	Total expenditures of federal awards				$ 5,036,234

See accompanying notes to schedule.

Graham County
Notes to schedule of expenditures of federal awards
Year ended June 30, 2016

Note 1 - Basis of presentation

The accompanying schedule of expenditures of federal awards (schedule) includes Graham County's federal grant activity for the year ended June 30, 2016. The information in this schedule is presented in accordance with the requirements of Title 2 U.S. Code of Federal Regulations (CFR) Part 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* (Uniform Guidance).

Note 2 - Summary of significant accounting policies

Expenditures reported on the schedule are reported on the modified accrual basis of accounting. Such expenditures are recognized following the cost principles contained in the Uniform Guidance, wherein certain types of expenditures are not allowable or are limited as to reimbursement. Therefore, some amounts presented in this schedule may differ from amounts presented in, or used in the preparation of, the financial statements.

Note 3 - Catalog of Federal Domestic Assistance (CFDA) numbers

The program titles and CFDA numbers were obtained from the federal or pass-through grantor or the 2016 *Catalog of Federal Domestic Assistance*.

Note 4 - Indirect cost rate

The County did not elect to use the 10 percent de minimis indirect cost rate as covered in 2 CFR §200.414.

This page is intentionally left blank.

COUNTY RESPONSE

Graham County Board of Supervisors
921 Thatcher Blvd • Safford, AZ 85546
Phone: (928) 428-3250 • Fax: (928) 428-5951

Danny Smith, Chairman
James A. Palmer, Vice Chairman
Paul David, Member

Terry Cooper, County Manager/Clerk

March 30, 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* 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* (Uniform Guidance). Specifically, for each finding we are providing you with the names of the contact people responsible for corrective action, the corrective action planned, and the anticipated completion date.

Sincerely,

Julie Rodriguez
Chief Financial Officer

Graham County
Corrective action plan
Year ended June 30, 2016

Financial statement findings

2016-01
The County should establish procedures to accurately record and report financial information
Contact Person: Julie Rodriguez, Chief Financial Officer
Anticipated completion date: June 30, 2018

Corrective Action: We concur with the finding. We do not disagree with the recommendation that a detailed review of the annual financial audit should be performed prior to submission. However, Graham County has been severely hampered by structural imbalances in our finances that we have been facing since 2008. We agree that hiring an additional finance person or a consultant with GAAP knowledge and financial statement preparation experience would be beneficial. However, due to our financial condition, we are unable to do so. We will review financial statements, as closely as possible, as we have no intention nor desire to include misstatements, omissions or errors in our financial statements. We will work to develop and draft a comprehensive written policy and procedure for compiling and presenting financial data within the annual financial report. In addition, we will try to find a resource person, perhaps in another county, willing and able to perform a review of financial statements prior to submission.

2016-02
The County should improve its policies and procedures over purchasing
Contact Person: Julie Rodriguez, Chief Financial Officer
Anticipated completion date: June 30, 2018

Corrective Action: While we concur with the finding, we believe the purchases noted were made in the best interest of the County and its constituents. We do, however, recognize the lack of documentation. We will work to revise a purchasing policy that includes requirements to document such situations as noted in this finding (including documenting selection of vendors other than the low bidder, sole source vendor documentation, emergency purchase documentation and subsequent board reporting and documenting the performance of due diligence when purchasing on state contract). We will communicate this policy to department heads and we will make every effort to provide for proper documentation in the future.

2016-03
The County should improve access controls over its information technology resources
Contact Person: John Lucas, IT Director
Anticipated completion date: June 2017

Graham County
Corrective action plan
Year ended June 30, 2016

Corrective Action: We concur with the finding. To help prevent and detect unauthorized access to IT resources 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.

- The County is in the process of approving IT user access and data center access policies.
- The County is in the process of approving a policy for physical access to data centers.
- The County is in the process of completing the configuration of logging software to monitor activities of users and users with elevated access.
- As noted in the draft User Access policy, IT will review all user accounts, including key users, twice annually.

2016-04
The County should improve its configuration management processes over its information technology resources
Contact Person: John Lucas, IT Director
Anticipated completion date: October 2017

Corrective Action: We concur with the finding. 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.

- The Change Management policy and related procedures are currently being drafted with an estimated completion date of October 2017. The policy will include processes covering all aspects of change management from rolling back changes, testing changes, and reviewing changes. The policy will address the separation of change management responsibilities. All items in policy will be logged for documentation.
- A server management policy to appropriately configure IT resources is currently in draft form. The County is in the process of approving the policy.

2016-05
The County should improve its risk-assessment process to include information technology security
Contact Person: John Lucas, IT Director
Anticipated completion date: June 2018

Corrective Action: We concur with the finding.

- The county will perform an IT risk assessment.
- A policy for information security is in process with an estimated completion date of December 2017.

Graham County
Corrective action plan
Year ended June 30, 2016

2016-06
The County should improve its contingency planning procedures for its information technology resources
Contact Person: John Lucas, IT Director
Anticipated completion date: August 2017

Corrective Action: We concur with the finding.

- The County is in the process of upgrading the IT disaster recovery plan and backup policy.
- The County will continue to improve our 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.
- Training for IT staff covering their responsibilities and roles will be conducted annually before each planned test.
- A table-top test of the County's failover site is planned for July 2017.
- The County plans a full-scale test of the equipment before August 2017.

2016-07
The County should improve security over its information technology resources
Contact Person: John Lucas, IT Director
Anticipated completion date: December 2017

Corrective Action: We concur with the finding. 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 will continue its efforts to ensure policies and procedures over it security are documented.

- The County has partially configured Netwrix Auditing software (July 2016) to log changes to Active Directory and users' activities accessing server files. The following reports are emailed to the Administrator on a daily basis: Active Directory Change Summary, Inactive Users in Active Directory, and Files Servers Change Summary.
- Cyber-security, safe personal training, and security awareness training for all employees has been prepared and is expected to begin in April 2017.
- Configuration and implementation of Windows Server Update Services (WSUS) to track and apply patches in a timely manner is anticipated by June 2017.
- The County will have a process in place over the next year to perform vulnerability scans.
- Incident response is being developed with the contingency plan and is expected to be completed by August 2017.
- The various policies that IT is currently drafting and will adopt over the next year are based on best practices. On an annual basis, IT will train and update IT staff on both current and new best practices encompassed within IT policies and procedures adopted by the County.

Graham County Board of Supervisors
921 Thatcher Blvd • Safford, AZ 85546
Phone: (928) 428-3250 • Fax: (928) 428-5951

Danny Smith, Chairman
James A. Palmer, Vice Chairman
Paul David, Member

Terry Cooper, County Manager/Clerk

March 30, 2017

Debbie Davenport
Auditor General
2910 N. 44th St., Ste. 410
Phoenix, AZ 85018

Dear Ms. Davenport:

We have prepared the accompanying summary schedule of prior audit findings as required 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* (Uniform Guidance). Specifically, we are reporting the status of audit findings included in the prior audit's schedule of findings and questioned costs. This schedule also includes the status of audit findings reported in the prior audit's summary schedule of prior audit findings that were not corrected.

Sincerely,

Julie Rodriguez
Chief Financial Officer

Graham County
Summary schedule of prior audit findings
Year ended June 30, 2016

Status of financial statement findings

The County should improve access controls over its information technology resources
Finding no.: 2015-01
Status: Partially corrected.
The County has performed the following:

- Implemented an IT administrative policy on October 5, 2015.
- Implemented a password policy on all county-owned equipment on February 11, 2016.
- Removed terminated employees' access that was identified during the FY 2015 audit.
- Updated termination forms to now require HR signature which assists with removing users' access immediately upon termination.
- Reviewed and removed shared, contractor, nonentity accounts.
- Modified generic access accounts by either disabling or locking to specific workstations.
- Removed all unnecessary administrator access accounts in October 2015.
- Verified that all VPN accounts with access to the County's network are only accessible by necessary in October 2015.

The reason for the finding's recurrence is the time frame between audit issuance and the end of the subsequent fiscal year (3/30/16 - 6/30/16) was inadequate to complete all pending items. The remaining planned action items are to complete, issue and implement the user access policies and the server/network policies.

- The County is in the process of approving IT user access and data center access policies.
- The County is in the process of approving a policy for physical access to data centers.
- The County is in the process of completing the configuration of logging software to monitor activities of users and users with elevated access.
- As noted in the draft User Access policy, IT will review all user accounts, including key users, twice annually.

The County should improve its information technology change management processes
Finding no.: 2015-02
Status: Partially corrected.
The policies for change management processes are in the draft stage of development. Changes to IT resources, including network devices (since December 2012) and servers (since March 2015), are manually documented in files accessible by IT staff with permission to make said changes.

The reason for the finding's recurrence is the time frame between audit issuance and the end of the subsequent fiscal year (3/30/16 - 6/30/16) was inadequate to complete all pending items. The remaining planned action items are to complete, issue and implement the change management process policies.

- The Change Management policy and related procedures are currently being drafted with an estimated completion date of October 2017. The policy will include processes covering all aspects of change management from rolling back changes, testing changes, and reviewing changes. The policy will address the separation of change management responsibilities. All items in policy will be logged for documentation.
- A server management policy to appropriately configure IT resources is currently in draft form.

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

Finding no.: 2015-03

Status: Partially corrected.

In June 2016 Graham County added a VM Server System four miles from the main location for server redundancy. All critical county services are replicated to this location at 15-minute intervals. In addition, the County services' servers are backed up to this location every night.

The reason for the finding's recurrence is the time frame between audit issuance and the end of the subsequent fiscal year (3/30/16 - 6/30/16) was inadequate to complete all pending items. The remaining planned action items is to complete, issue and implement the disaster recovery plan policies.

- The County is in the process of upgrading the IT disaster recovery plan and backup policy.
- The County will continue to improve our 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.
- Training for IT staff covering their responsibilities and roles will be conducted annually before each planned test.
- A table-top test of the County's failover site is planned for July 2017.
- The County plans a full-scale test of the equipment before August 2017.

The County should improve security over its information resources

Finding no.: 2015-04

Status: Partially corrected.

- The Acceptable Use Agreement Policy #2-2015 has been signed by all County employees. Graham County PC workstations users do not have administrative privilege to install apps or software.
- The County has partially configured Netwrix Auditing software (July 2016) to log changes to Active Directory and users' activities accessing server files. The following reports are emailed to the Administrator on a daily basis: Active Directory Change Summary, Inactive Users in Active Directory, and Files Servers Change Summary.

Graham County
Summary schedule of prior audit findings
Year ended June 30, 2016

The reason for the finding's recurrence is the time frame between audit issuance and the end of the subsequent fiscal year (3/30/16 - 6/30/16) was inadequate to complete all pending items. The remaining planned action items is to complete, issue and implement the server management policies and to finalize materials for the security awareness training and implement a Countywide training plan.

- Cyber-security, safe personal training, and security awareness training for all employees has been prepared and is expected to begin in April 2017.
- Configuration and implementation of Windows Server Update Services (WSUS) to track and apply patches in a timely manner is anticipated by June 2017.
- The County will have a process in place over the next year to perform vulnerability scans.
- Incident response is being developed with the contingency plan and is expected to be completed by August 2017.
- The various policies that IT is currently drafting and will adopt over the next year are based on best practices. On an annual basis, IT will train and update IT staff on both current and new best practices encompassed within IT policies and procedures adopted by the County.

Status of federal award findings and questioned costs

CFDA no. and program name: 97.042 **Emergency Management Performance Grants**
Finding no.: 2015-101
Status: Fully corrected.

CFDA no. and program name: 97.042 **Emergency Management Performance Grants**
Finding no.: 2014-101
Status: Fully corrected.


ARIZONA
Auditor General
Making a Positive Difference