Graham County

Single Audit Report

Year Ended June 30, 2017

A Report to the Arizona Legislature

ARIZONA Auditor General

Making a Positive Difference

ARIZONA Auditor General

Making a Positive Difference

The Arizona Office of the Auditor General's mission is to provide independent and impartial information and specific recommendations to improve the operations of state and local government entities. To this end, the Office provides financial audits and accounting services to the State and political subdivisions, investigates possible misuse of public monies, and conducts performance audits and special reviews of school districts, state agencies, and the programs they administer.

The Joint Legislative Audit Committee

Representative **Anthony Kern**, Chair

Representative **John Allen**

Representative **Rusty Bowers**

Representative **Rebecca Rios**

Representative **Athena Salman**

Representative **J.D. Mesnard** (ex officio)

Senator **Bob Worsley**, Vice Chair

Senator **Sean Bowie**

Senator **Judy Burges**

Senator **Lupe Contreras**

Senator **John Kavanagh**

Senator **Steve Yarbrough** (ex officio)

Audit Staff

Jay Zsorey, Director

Kathleen Wood, Manager and Contact Person

Contact Information

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

(602) 553-0333

www.azauditor.gov

TABLE OF CONTENTS

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

Independent auditors' report on internal control over financial reporting and on compliance and other matters based on an audit of basic financial statements performed in accordance with *Government Auditing Standards*

Members of the Arizona State Legislature

The Board of Supervisors
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, 2017, and the related notes to the financial statements, which collectively comprise the County's basic financial statements, and have issued our report thereon dated March 30, 2018.

Internal control over financial reporting

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

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies, and therefore, material weaknesses or significant deficiencies may exist that have not been identified. However, as described in the accompanying schedule of findings and questioned costs, 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 questioned costs as items 2017-02 and 2017-05 to be material weaknesses.

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the deficiencies described in the accompanying schedule of findings and questioned costs as items 2017-01, 2017-03, 2017-04, and 2017-06 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
Director, Financial Audit Division

March 30, 2018

STATE OF ARIZONA
OFFICE OF THE
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, 2017. 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 each of its major federal programs for the year ended June 30, 2017.

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, 2017, 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, 2018, 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
Director, Financial Audit Division

March 30, 2018


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 weaknesses identified?	**Yes**
Significant deficiencies identified?	**Yes**
Noncompliance material to the financial statements noted?	**No**

Federal awards

Internal control over major programs	
Material weaknesses identified?	**No**
Significant deficiencies 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

2017-01

The County should develop detailed financial statement preparation policies and procedures

Criteria—The County should have detailed policies and procedures to help ensure that its annual financial report, which 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).

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, the County did not properly record indirect costs as interfund reimbursements. Consequently, general government expenses/expenditures and charges for services revenues for governmental activities and the general fund were overstated by nearly $498,000. In addition, the County incorrectly recorded capital grants and contributions of approximately $435,200, misclassified expenses for pension-related claims and judgments payable of approximately $440,500, which was also omitted from the long-term liabilities note disclosure, and made several errors to various notes to financial statements. The County corrected most of these errors.

Effect—Without detailed policies and procedures and a thorough review, there is an increased risk that the County's annual financial report could contain misstatements and omit required information.

Cause—The County had limited staff and resources and, therefore, had not developed written policies and procedures to accurately prepare and perform a thorough review of its annual financial report. In addition, the County did not have documented procedures to record indirect costs as interfund reimbursements or otherwise eliminate the effects of recording interfund revenues and expenditures.

Recommendation—To help ensure that the County's annual financial report is accurate, complete, and prepared in accordance with GAAP, the County should:

- Develop and implement detailed written policies and procedures for compiling and presenting financial data within its annual financial report. These policies and procedures should include 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.
- Require an employee who is knowledgeable of GAAP and independent of the annual financial report's preparation to perform a detailed review to help ensure the annual financial report is accurate, complete, and presented in accordance with GAAP.
- Develop and implement documented procedures to properly record indirect costs as interfund reimbursements, which increase expenditures of the funds responsible for the expenditures and decrease expenditures of the funds that initially paid for the indirect costs. These procedures should require someone other than the preparer to review and approve these journal entries. Alternatively, these procedures could include a process for eliminating the effects of recording interfund revenues and expenditures.

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

This finding is similar to prior-year finding 2016-01.

2017-02

The County should improve access controls over its information technology resources

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

Condition and context—The County has written policies and procedures for managing access to its IT resources; however, they lacked critical elements, and the County did not consistently implement its policies and procedures to help prevent or detect unauthorized or inappropriate access to its IT resources.

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

Cause—The County had some documented policies and procedures and processes in place; however, the County did not compare them against IT standards and best practices, and they were not comprehensive and sufficiently detailed to ensure they were followed.

Recommendation—To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the County needs to further develop its logical and physical access policies and procedures over its IT resources. The County should review these policies and procedures against current IT standards and best practices, update them where needed, and implement them county-wide, as appropriate. Further, the County should train staff on the policies and procedures. The information below provides guidance and best practices to help the County achieve this objective.

- **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. Also, when an employee's job responsibilities change, a review of their access should be performed to ensure their access is compatible with the new 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 only be used 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 at the end of this report.

This finding is similar to prior-year findings 2016-03.

2017-03

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 written policies and procedures for managing changes to its IT resources to ensure changes were properly documented, authorized, reviewed, 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 and did not compare them against IT standards and best practices.

Recommendation—To help prevent and detect unauthorized, inappropriate, and unintended changes to its IT resources, the County needs to develop configuration management policies and procedures. The County should review these policies and procedures against current IT standards and best practices and implement them county-wide, as appropriate. Further, the County should train staff on the policies and procedures. The information below provides guidance and best practices to help the County achieve this objective.

- **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 systems 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 and maintain configuration settings—**Configure IT resources appropriately and securely, which includes limiting the functionality to ensure only essential services are performed, and maintain configuration settings for all systems.

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

This finding is similar to prior-year findings 2016-04.

2017-04

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

Criteria—The County faces risks of reporting inaccurate financial information and exposing sensitive data. An effective internal control system should include an entity-wide risk-assessment process that involves members of the County's administration and IT management to determine the risks the County faces as it seeks to achieve its objectives to report accurate financial information and protect sensitive data. An effective risk-assessment process provides the basis for developing appropriate risk responses and should include defining objectives to better identify risks and define risk tolerances, and identifying, analyzing, and responding to identified risks.

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

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

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

Recommendation—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.
- **Evaluate the impact disasters or other system interruptions could have on critical IT resources—**The evaluation should identify key business processes and prioritize the resumption of these functions within time frames acceptable to the entity in the event of contingency plan activation. Further, the results of the evaluation should be considered when updating its disaster recovery plan.

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

This finding is similar to prior-year findings 2016-05.

2017-05

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 because 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.

Recommendation—To help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources, the County needs to further develop its IT

security policies and procedures. The County should review these policies and procedures against current IT standards and best practices, update them where needed, and implement them county-wide, as appropriate. Further, the County should train staff on the policies and procedures. The information below provides guidance and best practices to help the County achieve this objective.

- **Perform proactive logging and log monitoring—**Key user and system activity should be logged, 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 and 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 the County's other departments to help eliminate similar vulnerabilities.
- **Apply patches—**Patches to IT resources should be evaluated, tested, and applied in a timely manner once the vendor makes them available.
- **Secure unsupported software—**Establish a strategy for assessing and securing any software that the manufacturer no longer updates and supports.
- **Protect sensitive or restricted data—**Restrict access to media containing data the entity, federal regulation, or state statute identifies as sensitive or restricted. Such media should be appropriately marked indicating the distribution limitations and handling criteria for data included on the media. In addition, media should be physically controlled and secured until it can be destroyed or sanitized using sanitization mechanisms with the strength and integrity consistent with the data's security classification.
- **Develop and document a process for awarding IT vendor contracts—**A process should be developed and documented to ensure the consideration of IT risks, costs, benefits, and technical specifications prior to awarding IT vendor contracts. In addition, contracts should include specifications addressing the management, reliability, governance, and security of the entity's IT resources. Further, for cloud services, ensure service contracts address all necessary security requirements based on best practices, such as physical location of data centers. Finally, IT vendors' performance should be monitored to ensure conformance with vendor contracts.

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

This finding is similar to prior-year findings 2016-07.

2017-06

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 had documented policies and procedures in place for performing system and data backups, it did not have documented policies and procedures for testing them to ensure they were operational and could be used to restore its IT resources.

Effect—The County risks not being able to provide for the continuity of operations, recover vital IT systems and data, and conduct daily operations in the event of a disaster, system or equipment failure, or other interruption, which could cause inaccurate or incomplete system and data recovery.

Cause—The County had some documented policies and procedures and processes in place but lacked a sufficiently documented and updated contingency plan and did not compare its policies and procedures and contingency plan to current IT standards and best practices.

Recommendation—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 County should review its contingency planning procedures against current IT standards and best practices, update them where needed, and implement them county-wide as appropriate. Further, the County should train staff on the policies and procedures. The information below provides guidance and best practices to help the County achieve this objective.

- **Update the contingency plan and ensure it includes all required elements to restore operations—** Contingency plans should be updated at least annually for all critical information or when changes are made to IT resources, and updates to the plan should be communicated to key personnel. The plan should include essential business functions and associated contingency requirements, including 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 the County's other plans such as its continuity of operations, cyber incident response, and emergency response plans. Plan testing may include actual tests, simulations, or tabletop 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.

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

This finding is similar to prior-year findings 2016-06.

Federal award findings and questioned costs

None reported.

COUNTY SECTION

Graham County
Schedule of expenditures of federal awards
Year ended June 30, 2017

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 (NSLP)	Child Nutrition Cluster	Arizona Department of Education	None	$ 22,939
10 557	WIC Special Supplemental Nutrition Program for Women, Infants, and Children		Arizona Department of Health Services	ADHS14-053054	200,058
10 665	Schools and Roads—Grants to States	Forest Service Schools and Roads Cluster	Arizona State Treasurer	None	57,861
	Total Department of Agriculture				280,858
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	117-14	134,355
Department of the Interior					
15 226	Payments in Lieu of Taxes				2,866,774
Department of Justice					
16 575	Crime Victim Assistance		Arizona Department of Public Safety	2014-VA-GX-0018	14,518
16 606	State Criminal Alien Assistance Program				371
16 607	Bulletproof Vest Partnership Program				13,142
16 738	Edward Byrne Memorial Justice Assistance Grant Program				7,651
16 738	Edward Byrne Memorial Justice Assistance Grant Program		Arizona Criminal Justice Commission	DC-17-024, DC-17-005	29,179
	Total 16.738				36,830
	Total Department of Justice				64,861
Department of Transportation					
20 205	Highway Planning and Construction (Federal-Aid Highway Program)	Highway Planning and Construction Cluster	Arizona Department of Transportation	P0012013000786	89,935
20 616	National Priority Safety Programs	Highway Safety Cluster	Governor's Office of Highway Safety	2017-II-007, 2017-PT-025, 2017-405d-043	52,016
	Total Department of Transportation				141,951
Department of Education					
84 010	Title I Grants to Local Educational Agencies (LEAs)		Arizona Department of Education	17FT1TTI-713185-01A	14,404
84 027	Special Education—Grants to States	Special Education Cluster (IDEA, Part B)	Arizona Department of Education	17FESCBG-713185-09A, 17FESSCG-713189-55B	508,261
84 027	Special Education—Grants to States	Special Education Cluster (IDEA, Part B)	Arizona Supreme Court	17FESCBG-713225-09A, 17FESSCG-713225-55B	8,762
	Total 84.027				517,023
84 173	Special Education—Preschool Grants	Special Education Cluster (IDEA Preschool)	Arizona Department of Education	17FECCBP-713185-37A	19,597
	Total Special Education Cluster (IDEA)				536,620
84 358	Rural Education			N/A	16,930
84 367	Supporting Effective Instruction State Grants (formerly Improving Teacher Quality State Grants)		Arizona Department of Education	17FT1TII-713185-03A	1,760
	Total Department of Education				569,714

See accompanying notes to schedule.

Graham County
Schedule of expenditures of federal awards
Year ended June 30, 2017

Federal agency/CFDA number	Federal program name	Cluster title	Pass-through grantor	Pass-through grantor's numbers	Program expenditures
Department of Health and Human Services					
93 069	Public Health Emergency Preparedness		Arizona Department of Health Services	ADHS17-133191	201,256
93 074	Hospital Preparedness Program (HPP) and Public Health Emergency Preparedness (PHEP) Aligned Cooperative Agreements		Arizona Department of Health Services	ADHS17-133191	11,162
93 323	Epidemiology and Laboratory Capacity for Infectious Diseases (ELC)		Arizona Department of Health Services	ADHS17-133191	32,355
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	77,470
93 758	Preventive Health and Health Services Block Grant funded solely with Prevention and Public Health Funds (PPHF)		Arizona Department of Health Services	ADHS16-098358	1,252
93 940	HIV Prevention Activities—Health Department Based		Arizona Department of Health Services	ADHS13-031211	6,076
93 945	Assistance Programs for Chronic Disease Prevention and Control		Arizona Department of Health Services	ADHS17-149140	9,121
93 977	Sexually Transmitted Diseases (STD) Prevention and Control Grants		Arizona Department of Health Services	ADHS14-068669	8,435
93 994	Maternal and Child Health Services Block Grant to the States		Arizona Department of Health Services	ADHS16-098358	67,550
	Total Department of Health and Human Services				414,677
Department of Homeland Security					
97 042	Emergency Management Performance Grants		Arizona Department of Emergency and Military Affairs	EMF-2016-EP-00009-S01	46,209
97 067	Homeland Security Grant Program		Arizona Department of Emergency and Military Affairs	140308-01, 150308-01, 160306-01	101,561
	Total Department of Homeland Security				147,770
	Total expenditures of federal awards				$ 4,620,960

See accompanying notes to schedule.

Graham County
Notes to schedule of expenditures of federal awards
Year ended June 30, 2017

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, 2017. 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 2017 *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, 2018

Jay Zsorey
Auditor General
2910 N. 44th St., Ste. 410
Phoenix, AZ 85018

Dear Mr. Zsorey:

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 our responsible officials' views, 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, 2017

Financial statement findings

2017-01
The County should develop detailed financial statement preparation policies and procedures
Contact person: Julie Rodriguez, Chief Financial Officer
Anticipated completion date: June 2019

Corrective action: We concur with the finding.

- As CFO, I will continue to develop and implement detailed written policies and procedures for compiling and presenting information within the annual financial report. These written procedures will include instructions for compiling and obtaining information both from within the County's accounting system as well as information not readily available.
- During the 2019 budget process, we will work to budget for hiring additional finance personnel with a knowledge of GAAP to perform a detailed review of the annual financial report to ensure the report is accurate, complete and presented in accordance with GAAP.
- The process for recording the indirect cost transaction noted in this finding was corrected in March 2018 and is now correctly processed as an interfund reimbursement. This journal entry will follow the County's standard procedures, and will be approved by the County Manager.

2017-02
The County should improve access controls over its information technology resources
Contact person: McCoy Hawkins, IT Director
Anticipated completion date: June 2019

Corrective action: We concur with the finding and are anticipating new software to be implemented July 1, 2018 to phase out current Treasurer's program. This new software will improve access controls by allowing rights to be assigned and authenticated by Active Directory groups. Legacy resources and permissions are currently being reviewed and phased out if necessary to comply with active policies and procedures in order to help prevent inappropriate access to IT resources.

2017-03
The County should improve its configuration management processes over its information technology resources
Contact person: McCoy Hawkins, IT Director
Anticipated completion date: June 2019

Corrective action: We concur with the finding and are currently drafting Change Management and related policies and procedures. These policies will include processes covering all aspects of change management from testing changes, rolling back changes, and reviewing changes, including emergency changes, based upon current IT standards and best practices. The policy will address the separation of change management responsibilities and outline training of proper personnel about those responsibilities. All items in policy will be logged for documentation.

2017-04
The County should improve its risk-assessment process to include information technology security
Contact person: McCoy Hawkins, IT Director
Anticipated completion date: June 2019

Corrective action: We concur with the finding and will perform an IT risk assessment to identify, analyze, and respond to risks that may impact our IT resources. A policy for information management and security is in process, along with various other policies being drafted based on best practices and in collaboration with other counties.

2017-05
The County should improve security over its information technology resources
Contact person: McCoy Hawkins, IT Director
Anticipated completion date: June 2019

Corrective action: We concur with the finding and are in collaboration with other counties to develop security policies and procedures based on current IT standards and best practices. Mandatory staff trainings will be held annually to provide basic understanding of information security and security awareness.

2017-06
The County should improve its contingency planning procedures for its information technology resources
Contact person: McCoy Hawkins, IT Director
Anticipated completion date: June 2019

Corrective action: We concur with the finding and are in process of upgrading the IT disaster recovery plan and backup policies, 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. Incident response and training is being developed with this contingency plan.

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, 2018

Jay Zsorey
Auditor General
2910 N. 44th St., Ste. 410
Phoenix, AZ 85018

Dear Mr. Zsorey:

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, 2017

The County should establish procedures to accurately record and report financial information
Finding no.: 2016-01
Status: Partially corrected.

- We did review financial statements as closely as possible and we have begun but will continue to work toward developing a written policy and procedure for compiling and presenting financial data within the annual financial report.
- We were not financially able to hire an additional finance person or consultant with GAAP knowledge and financial preparation experience by the previous anticipated completion date of June 30, 2018. We also were unable to find a resource person outside the county willing and able to perform a review prior to submission.
- During the 2019 budget process, we will work to budget for hiring additional finance personnel with an estimated completion date of June 30, 2019.
- The reason for the finding's recurrence is budget limitations during the fiscal year continued to prevent us from hiring additional finance personnel.

The County should improve its policies and procedures over purchasing
Finding no.: 2016-02
Status: Partially corrected.

- We did increase our efforts to document purchases to show required steps were followed.
- We are still in the process of revising our current purchasing policy to include documenting of purchasing requirements. We anticipate having this policy completed within the 2018 fiscal year and we will communicate the new policy to department heads and make every effort to provide for proper documentation in the future.
- The reason for the finding's recurrence is lack of personnel to revise the purchasing policy within the time period in which we had intended.

The County should improve access controls over its information technology resources
Finding no.: 2015-01, 2016-03
Status: Partially Corrected

- The County's User Access Administrative Policy #2-2017 was approved May 15, 2017.
- IT policies and procedures for Strategic Facilities Access outlining physical access to data centers was approved March 23, 2017.
- Netwrix Auditor software logs activities and changes made to all active directory user accounts, with notifications of elevated access alterations.
- As specified in the Users Access Administrative Policy #2-2017, all user accounts are verified with employment and contract status a minimum of twice a year. VPN accounts are also reviewed to verify they are still active and necessary.

- New software is projected to be implemented July 1, 2018 to phase out current Treasurer's program. This new software will improve access controls by allowing rights to be assigned and authenticated by Active Directory groups.
- The reason for the finding's recurrence is lack of personnel and County resources to remove all legacy programs and permissions, and configure new software within the time frame given.

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

Finding no.: 2015-02, 2016-04

Status: Partially corrected.

- IT Policies and Procedures for Server Management was approved March 23, 2017.
- The Change Management policy and related procedures are currently being drafted with a goal to be completed by the end of June 2019. The policy will include processes covering all aspects of change management from testing changes, rolling back changes, and reviewing changes. The policy will address the separation of change management responsibilities and outline training of proper personnel about those responsibilities. All items in policy will be logged for documentation.
- The reason for the finding's recurrence is lack of personnel to draft the necessary policies and procedures within the time frame given.

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

Finding no.: 2015-04, 2016-05, 2016-07

Status: Partially corrected.

- The County's User Access Administrative Policy #2-2017 which was approved May 15, 2017, was distributed and signed by all users.
- Netwrix Auditor software logs activities and changes made to all active directory user accounts, with notifications of elevated access alterations and daily Active Directory Change Summary report.
- A mandatory Cyber-Security training was held April 2017, and an online version is required by all new employees. In September 2016, Safe-Personnel online trainings were implemented for new employees to complete all trainings required by their position.
- Windows Server Update Services (WSUS) was implemented May 2017 to track and apply patches on all domain devices in a timely manner.
- In addition to the anti-virus and anti-malware software on all devices, and Advanced Threat Protection on the web filters, an Intrusion Prevention System module was added to the firewall in October 2016 to also perform vulnerability scans.
- The County will perform an IT risk assessment to identify, analyze, and respond to risks that may impact our IT resources. A policy for information management and security is in process, along with various other policies being drafted based on best practices and in collaboration with other counties with a goal to be completed by the end of June 2019.

- The reason for the finding's recurrence is lack of personnel and County resources to perform the risk-assessment and draft the required policies and procedures within the time frame given.

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

Finding no.: 2015-03, 2016-06

Status: Partially corrected.

- On June 17, 2017, a test of the New World offsite virtual machine redundancy was successful, and further testing of other servers and outages are planned prior to June 2018.
- The County is in process of upgrading the IT disaster recovery plan and backup policies, 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. Incident response and training is being developed with this contingency plan which is projected to be completed by June 2019.
- The reason for the finding's recurrence is lack of personnel and County resources to update and draft necessary policies and procedures within the time frame given.


ARIZONA
Auditor General
Making a Positive Difference