Santa Cruz County

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

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
David Glennon, 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

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

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

Members of the Arizona State Legislature

The Board of Supervisors of
Santa Cruz 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, business-type activities, each major fund, and aggregate remaining fund information of Santa Cruz 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 23, 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 2017-01 through 2017-04 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 2017-05 through 2017-07 to be significant deficiencies.

Compliance and other matters

As part of obtaining reasonable assurance about whether the County's basic financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed an instance of noncompliance or other matter that is required to be reported under *Government Auditing Standards* and that is described in the accompanying schedule of findings and questioned costs as item 2017-06.

Santa Cruz County response to findings

Santa Cruz 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 23, 2018

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 of
Santa Cruz County, Arizona

Report on compliance for each major federal program

We have audited Santa Cruz 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 qualified and unmodified opinions on compliance for major federal programs. However, our audit does not provide a legal determination of the County's compliance.

Basis for qualified opinion on the Homeland Security Grant Program

As described in the accompanying schedule of findings and questioned costs as item 2017-102, the County did not comply with the equipment and real property management compliance requirements for the Homeland Security Grant Program, CFDA number 97.067. Compliance with such requirements is necessary, in our opinion, for the County to comply with the requirements applicable to that program.

Qualified opinion on the Homeland Security Grant Program

In our opinion, except for the noncompliance described in the basis for qualified opinion paragraph, Santa Cruz County complied, in all material respects, with the types of compliance requirements referred to above that could have a direct and material effect on the Homeland Security Grant Program for the year ended June 30, 2017.

Unmodified opinion on each of the other major federal programs

In our opinion, Santa Cruz 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 other major federal programs identified in the summary of auditors' results section of the accompanying schedule of findings and questioned costs for the year ended June 30, 2017.

Other matters

The results of our auditing procedures disclosed an instance of noncompliance that is required to be reported in accordance with the Uniform Guidance and that is described in the accompanying schedule of findings and questioned costs as item 2017-101. Our opinion on each major federal program is not modified with respect to this matter.

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, and therefore, material weaknesses or significant deficiencies may exist that have not been identified. We identified certain deficiencies in internal control over compliance, as described in the accompanying schedule of findings and questioned costs as items 2017-101 and 2017-102, that we consider to be material weaknesses.

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.

Santa Cruz County response to findings

Santa Cruz 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 compliance, and accordingly, we express no opinion on them.

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

We have audited the financial statements of the governmental activities, business-type activities, each major fund, and aggregate remaining fund information of Santa Cruz 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 23, 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 23, 2018

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?	**Yes**
Significant deficiencies identified?	**None reported**

Type of auditors' report issued on compliance for major programs

Unmodified for Payments in Lieu of Taxes (15.226) and Public Health Emergency Preparedness (93.069); and qualified for the Homeland Security Grant Program (97.067)

Any audit findings disclosed that are required to be reported in accordance with 2 CFR §200.516(a)?	**Yes**

Identification of major programs

CFDA number	Name of federal program or cluster
15.226	Payments in Lieu of Taxes
93.069	Public Health Emergency Preparedness
97.067	Homeland Security Grant Program

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 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 relied on an informal process to perform risk-assessment 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.
- **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 evaluation results should be considered when developing its disaster recovery plan.

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

2017-02

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 relied on an informal process for controlling access to its IT resources.

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

- **Review user access—**A periodic, comprehensive review should be performed of all existing employee accounts to help ensure that network and system access granted is needed and compatible with job responsibilities.
- **Remove terminated employees' access to its IT resources—**Employees' network and system access should immediately be removed upon their terminations.
- **Review contractor and other nonentity account access—**A periodic review should be performed on contractor and other nonentity accounts with access to an entity's IT resources to help ensure their access remains necessary and appropriate.
- **Review all shared accounts—**Shared network access accounts should be reviewed and eliminated or minimized when possible.
- **Manage shared accounts—**Shared accounts should be used only when appropriate and in accordance with an established policy authorizing the use of shared accounts. In addition, account credentials should be reissued on shared accounts when a group member leaves.
- **Review and monitor key activity of users—**Key activities of users and those with elevated access should be reviewed for propriety.
- **Improve network and system password policies—**Network and system password policies should be improved and ensure they address all accounts.
- **Manage employee-owned and entity-owned electronic devices connecting to the network—**The use of employee-owned and entity-owned electronic devices connecting to the network should be managed, including specifying configuration requirements and the data appropriate to access; inventorying devices; establishing controls to support wiping data; requiring security features, such as passwords, antivirus controls, file encryption, and software updates; and restricting the running of unauthorized software applications while connected to the network.

- **Manage remote access**—Security controls should be utilized for all remote access. These controls should include appropriate configuration of security settings such as configuration/connections requirements and the use of encryption to protect the confidentiality and integrity of remote sessions.
- **Review data center access**—A periodic review of physical access granted to the data center should be performed to ensure that it continues to be needed.

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

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

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 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 relied on an informal process for making changes to its IT resources.

Recommendations—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 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.
- **Rollback 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.
- **Manage software installed on employee computer workstations—**For software installed on employee computer workstations, policies and procedures should be developed to address what software is appropriate and the process for requesting, approving, installing, monitoring, and removing software on employee computer workstations.

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

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

2017-04

The County should improve security over its information technology resources

Criteria—The selection and implementation of security controls for the County's information technology (IT) resources, which include its systems, network, infrastructure, and data, are important 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 includes 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 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 relied on an informal process for security over its IT resources.

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

security policies and procedures. The County should review these policies and procedures against current IT standards and best practices 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, 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 on-going 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.
- **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.

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

2017-05

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 did not have a written contingency plan. 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 had some contingency planning processes in place but lacks a sufficiently documented recovery plan based on current IT standards and best practices to ensure that its contingency efforts can be relied on in the event 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 develop and document its contingency planning procedures. The County should review its contingency planning procedures against current IT standards and best practices and implement them county-wide, as appropriate. The information below provides guidance and best practices to help the County achieve this objective.

- **Develop and implement a contingency plan—**A contingency plan should be developed and implemented and include essential business functions and associated contingency requirements; 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.
- **Move critical operations to a separate alternative site—**Policies and procedures should be developed and documented for migrating critical IT operations to a separate alternative site for essential business functions, including putting contracts in place or equipping the alternative site to resume essential business functions, if necessary. The alternative site's information security safeguards should be equivalent to the primary site.
- **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 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. 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 2016-05.

2017-06

The County Treasurer did not comply with state laws for apportioning interest earnings

Criteria—The County Treasurer's Office is responsible for managing and investing millions of dollars in public monies. Therefore, the County Treasurer's Office should apportion pooled interest earnings as specified in Arizona Revised Statutes, Titles 15 and 35.

Condition and context—At June 30, 2017, the County Treasurer's Investment Pool reported approximately $39.2 million of deposits and investments that included $9.7 million for Santa Cruz County and another $29.5 million for other political subdivisions, such as school districts. However, the County Treasurer's Office did not apportion interest earnings during the fiscal year to investment pool participants for the majority of its pooled investments as required by state laws.

Effect—The County Treasurer's Office did not ensure that pooled investment earnings were properly distributed to the various county funds and political subdivisions in accordance with state laws.

Cause—The County Treasurer's Office lacked comprehensive internal control policies and procedures over the apportionment of pooled interest earnings.

Recommendation—The County Treasurer's Office should improve its written policies and procedures to help ensure compliance with state laws for apportioning interest earnings to investment pool participants. Those policies and procedures should include, at a minimum, detailed instructions for apportioning interest earnings to pooled investment accounts on at least a quarterly basis and determining the amounts to be apportioned based on average monthly balances of pooled accounts.

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

This finding is similar to prior-year finding 2016-02.

2017-07

The County should improve its policies and procedures for preparing its annual financial statements and note disclosures

Criteria—The County should improve its policies and procedures over the preparation of its annual financial report to ensure its financial statements and related note disclosures are prepared in accordance with U.S. generally accepted accounting principles (GAAP). Accurate financial statements provide valuable information to those charged with governance, management, and other financial statement users to make important decisions about the County's financial operations.

Condition and context—The County did not have sufficient written policies and procedures over the preparation of its annual financial report to ensure its financial statements and related note disclosures were accurate and prepared in accordance with GAAP.

Effect—There is an increased risk that that the financial statements may contain material misstatements that range from clerical and mathematical errors to noncompliance with GAAP.

Cause—The County relied on an informal process for preparing its annual financial report.

Recommendation—To help ensure that the County's financial statements and related note disclosures are accurate and prepared in accordance with GAAP, the County should:

- Develop and implement comprehensive written policies and procedures for compiling the information and preparing its annual financial report. These procedures should include detailed instructions for obtaining information from the accounting system and information not readily available from the accounting system, but necessary for financial statement preparation.
- Require an employee who is independent of the person preparing the financial statements and knowledgeable of the County's operations and GAAP reporting requirements to review the statements and related note disclosures. This review should ensure that the amounts are accurate and properly supported and the County prepares the financial statements 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.

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

Federal award findings and questioned costs

2017-101

CFDA number and name: Not applicable
Questioned costs: N/A

Criteria—In accordance with 2 Code of Federal Regulations (CFR) §200.510(b), the County must prepare a schedule of expenditures of federal awards (SEFA) for the period covered by the financial statements. At a minimum, the SEFA must:

- List individual federal programs by federal agency. For a cluster of programs, the SEFA must also provide the cluster name, list individual federal programs within the cluster of programs, and provide the applicable federal agency name.
- For federal awards received as a subrecipient, include the name of the pass-through entity and identifying number assigned by the pass-through entity.
- Provide total federal awards expended for each individual federal program and the CFDA number or other identifying number when the CFDA information is not available. For a cluster of programs, the SEFA must also provide the total for the cluster.
- Include the total amount provided to subrecipients from each federal program.

Condition and context—The County did not prepare an accurate and complete SEFA. Specifically, the County failed to identify $242,968 as being provided to subrecipients for three federal programs. In addition, the County understated its federal award expenditures by $10,933 and made several mistakes in reporting the appropriate CFDA number and federal program title, the appropriate cluster names and totals, and the appropriate pass-through entity identifying information. The County's SEFA was adjusted for these errors.

Effect—The County's initial SEFA was not accurate and complete. This finding was not a result of internal control deficiencies of individual federal programs and, accordingly, did not have a direct and material effect on the reporting requirements over the County's major federal programs.

Cause—The County did not have effective policies and procedures in place to ensure that all federal monies, including monies passed through to subrecipients, were properly identified and reported on the SEFA.

Recommendation—To help ensure that the County prepares its SEFA in compliance with Uniform Guidance, the County should develop and implement an effective review process to ensure accurate and complete information is reported on the SEFA.

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 2016-101.

2017-102

CFDA number and name: 97.067 **Homeland Security Grant Program**

Award numbers and years: 15-AZDOHS-HSGP-150406-02, October 1, 2015 through December 31, 2016; 15-AZDOHS-OPSG-150417-01, January 1, 2016 through December 31, 2016; 16-AZDOHS-HSGP-160405-01, October 1, 2016 through September 30, 2017; 16-AZDOHS-OPSG-160420-01, November 1, 2016 through December 31, 2017

Federal agency: **U.S. Department of Homeland Security**

Pass-through grantor: **Arizona Department of Homeland Security**

Compliance requirement: Equipment and real property management

Questioned costs: None

Criteria—In accordance with 2 CFR §200.313 (c) and (d), the County must maintain property records that include a description of the property; a serial number or other identification number; the source of funding for the property; who holds the title; the acquisition date; cost of the property; percentage of federal

participation in the project costs for the federal award under which the property was acquired; the location, use, and condition of the property; and any ultimate disposition data including the date of disposal and sale price of the property. In addition, the County must develop a control system to ensure adequate safeguards to prevent loss, damage, or theft of property purchased with federal funds. Further, the County must use equipment in the program or project for which it was acquired as long as needed, whether or not the project or program continues to be supported by the federal award. When no longer needed for the original program or project, the equipment may be used in other activities supported by the federal awarding agency. Finally, the County is required by 2 CFR §200.303 to maintain effective internal control over its Homeland Security Grant Program to provide reasonable assurance that it is managing the award in compliance with federal statutes, regulations, and the award terms.

Condition and context—The County did not maintain effective control and accountability for prior-year equipment and vehicle purchases made with federal monies. For the Homeland Security Grant Program, the County maintains 61 capital assets purchased with federal program monies currently valued at $67,578. Specifically, the County's capital asset list did not include a unique identifier, such as a tag number or serial number, for 8 capital assets with a total value of $11,748. Further, for three vehicles selected, the County used the vehicles for basic law enforcement services for the community and they were no longer specifically dedicated for federal program use.

Effect—The County did not comply with federal regulations, and its failure to maintain control over capital assets purchased with federal grant monies could result in equipment and vehicles being lost, stolen, damaged, or not used for their intended purpose.

Cause—The County did not follow its policy for tagging equipment and ensuring that complete and accurate information for each asset is recorded in its capital asset list. Further, the County was under the impression that after 3 years of ownership, the vehicles purchased with federal grant monies could be used for any local county law enforcement purpose.

Recommendation—To help ensure compliance with federal regulations and to help prevent loss, theft, damage or misuse of capital assets purchased with federal monies, the County should ensure that its policies are followed that require all equipment items to be properly inventoried, tagged, and accounted for in its capital asset list. Further, the County should establish policies to ensure that equipment is used in the program or project for which it was acquired as long as needed, whether or not the project or program continues to be supported by the federal award.

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 2016-102.

COUNTY SECTION

Santa Cruz 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	Amount provided to subrecipients
Department of Agriculture						
10 665	Schools and Roads—Grants to States	Forest Service Schools and Roads Cluster			$ 30,203	
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	116-17	20,567	
Department of the Interior						
15 226	Payments in Lieu of Taxes				1,080,113	
15 227	Distribution of Receipts to State and Local Governments				2,064	
	Total Department of the Interior				1,082,177	
Department of Justice						
16 588	Violence Against Women Formula Grants		Arizona Governor's Office of Youth, Faith and Family	ST-WSG-15-010115-19Y2, ST-WSG-15-010115-19Y3	220,130	
16 738	Edward Byrne Memorial Justice Assistance Grant Program		Arizona Criminal Justice Commission	DC-17-032, DC-17-012	60,264	
	Total Department of Justice				280,394	
Department of Labor						
17 258	WIOA Adult Program	WIOA Cluster	Arizona Department of Economic Security	DI16-002111	205,522	
17 259	WIOA Youth Activities	WIOA Cluster	Arizona Department of Economic Security	DI16-002111	215,631	
17 278	WIOA Dislocated Worker Formula Grants	WIOA Cluster	Arizona Department of Economic Security	DI16-002111	137,931	
	Total WIOA Cluster				559,084	
17 274	YouthBuild		Pima County	CT-CS-15*20	271,358	$ 92,454
	Total Department of Labor				830,442	92,454
Department of Transportation						
20 106	Airport Improvement Program		Arizona Department of Transportation	E6F1P	329,416	
20 600	State and Community Highway Safety	Highway Safety Cluster	Arizona Governor's Office of Highway Safety	2016-AL-075, 2016-OP-020, 2016-PT-037, 2016-AL-038, 2017-PT-073, 2017-AL-040, 2017-OP-014, 2017-PT-053, 2017-PT-054	20,924	
20 703	Interagency Hazardous Materials Public Sector Training and Planning Grants		Arizona Emergency Response Commission	HM-HMP-0513-15-01-00, HM-HMP-0583-16-01-00	4,541	
	Total Department of Transportation				354,881	
Environmental Protection Agency						
66 931	International Financial Assistance Projects Sponsored by the Office of International and Tribal Affairs		Border Environment Cooperation Commission	TAA16-0111	11,034	

See accompanying notes to schedule.

Santa Cruz 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	Amount provided to subrecipients
Department of Education						
84 002	Adult Education—Basic Grants to States		Arizona Department of Education	17-FAEAPL-713397-16B, 17-FEDWIO-713397-16B, 17FAEABE-713397-16B, 17-FAEIEL-713397-16B	148,649	
84 010	Title I Grants to Local Educational Agencies		Arizona Department of Education	17-FLCCL-713341-02A	1,589	
84 027	Special Education—Grants to States	Special Education Cluster (IDEA)	Arizona Department of Education	17-FESCBG-713341-09A, 17-FESSCG-713341-55B	21,830	
84 215	Fund for the Improvement of Education				305,237	
84 367	Supporting Effective Instruction State Grant		Arizona Department of Education	17FT1TII-713341-03A	3,471	
	Total Department of Education				480,776	
Department of Health and Human Services						
93 008	Medical Reserve Corps Small Grant Program		National Association of County and City Health Officials	MRC 14-1874	1,245	
93 069	Public Health Emergency Preparedness		Arizona Department of Health Services	ADHS17-133199, ADHS17-133199:1, ADHS17-133199:2, ADHS12-007896:7	287,440	
93 074	Hospital Preparedness Program (HPP) and Public Health Emergency Preparedness (PHEP) Aligned Cooperative Agreements		Arizona Department of Health Services	ADHS12-007896:6	272	
93 268	Immunization Cooperative Agreements		Arizona Department of Health Services	ADHS13-041547:15, ADHS13-041547:22	7,479	7,479
93 323	Epidemiology and Laboratory Capacity for Infectious Diseases (ELC)		Arizona Department of Health Services	ADHS17-133199:4	30,574	
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	ADHS13-041547:16, ADHS13-041547:17, ADHS13-041547:18, ADHS13-041547:19, ADHS13-041547:20	143,035	143,035
93 563	Child Support Enforcement		Arizona Department of Economic Security	ADES13-035445	76,767	
93 667	Social Services Block Grant		Southeastern Arizona Governments Organization	121-17	83,837	
93 912	Rural Health Care Services Outreach, Rural Health Network Development and Small Health Care Provider Quality Improvement Program		Mariposa Community Health Center	D06RH21674	9,119	
93 959	Block Grants for Prevention and Treatment of Substance Abuse		Arizona Department of Health Services	IGA-SABG-GR-16-040116-13-1, IGA-SABG-GR-16-040116-13-2, IGA-SABG-GR-17-070116-13, IGA-SABG-GR-18-070117-12	48,584	
	Total Department of Health and Human Services				688,352	150,514

See accompanying notes to schedule.

Santa Cruz 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	Amount provided to subrecipients
Executive Office of the President						
95 001	High Intensity Drug Trafficking Areas Program		City of Tucson	HT-16-2628, HT-16-2629	327,278	
Department of Homeland Security						
97 042	Emergency Management Performance Grants		Arizona Department of Emergency and Military Affairs	EMF-2016-EP-00009-S01	125,928	
97 067	Homeland Security Grant Program		Arizona Department of Homeland Security	16-AZDOHS-HSGP-160405-01, 15-AZDOHS-HSGP-150406-02, 15-AZDOHS-OPSG-150417-01, 16-AZDOHS-OPSG-160420-01	586,478	
	Total Department of Homeland Security				712,406	
	Total expenditures of federal awards				$ 4,818,510	$ 242,968

See accompanying notes to schedule.

Santa Cruz 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 Santa Cruz 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*.

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) number

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 elected to use the 10 percent de minimis indirect cost rate as covered in 2 CFR §200.414.

COUNTY RESPONSE

ADMINISTRATIVE SERVICES
SANTA CRUZ COUNTY

Mauricio A. Chavez, CMPI
Director of Finance &
Administrative Services

March 23, 2018

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

Dear Ms. Davenport:

We have prepared the accompanying corrective action plan as required by the standards applicable to financial audits contained in *Government Auditing Standards* and by the audit requirements of Title 2 U.S. Code of Federal Regulations Part 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*. Specifically, for each finding we are providing you with our responsible officials' views, the names of the contact people responsible for corrective action, the corrective action planned, and the anticipated completion date.

Sincerely,

Mauricio A. Chavez
Director of Finance & Administrative Services

2150 North Congress Drive | P.O. Box 1150 | Nogales, Arizona 85621
(520) 375-7820 | FAX (520) 375-7819 | TDD (520) 761-7816

Santa Cruz County
Corrective action plan
Year ended June 30, 2017

Financial Statement Findings

2017-01

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

Responsible officials' view: The County concurs with this finding

Name(s) of contact person(s): Robert Heming, Information Technology Director
Anticipated completion date: September 30, 2018

Corrective Action: The County is in the process of identifying resources to perform vulnerability testing. Different disaster/risk IT scenarios will be developed and documented to address location-specific threats. The County will evaluate software to identify, classify, and inventory County data. The County will work to have a NIST compliant solution. The County will implement and test an off-site Disaster recovery solution that mirrors all systems in real time. The County will continue to work with the Auditor General's Office to adequately address potential risks to our resources.

2017-02

The County should improve access controls over its information technology resources

Responsible officials' view: The County concurs with this finding

Name(s) of contact person(s): Robert Heming, Information Technology Director
Anticipated completion date: March 31, 2019

Corrective Action: The County will implement an automated process to disable terminated employees. User security is reviewed quarterly and includes contractors, shared accounts, and internal users. The County is in the process of evaluating system/network auditing software to review user access. The County will implement audit event logs like security/system. The County will continue to work with the Auditor General's Office to adequately address our configuration management processes and potential risks to our resources.

Santa Cruz County
Corrective action plan
Year ended June 30, 2017

2017-03

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

Responsible officials' view: The County concurs with this finding

Name(s) of contact person(s): Robert Heming, Information Technology Director
Anticipated completion date: March 31, 2019

Corrective Action: The County will implement a Change Control Process that documents changes, testing fallback plans, and approval processes. The policies and procedures documentation will require additional time. The County will continue to work with the Auditor General's Office to adequately address our configuration management processes and potential risks to our resources.

2017-04

The County should improve security over its information technology resources

Responsible officials' view: The County concurs with this finding

Name(s) of contact person(s): Robert Heming, Information Technology Director
Anticipated completion date: March 31, 2019

Corrective Action: The County will implement processes to patch systems and software on a regular basis. The County is the process of evaluating software to perform proactive logging, monitoring and auditing. The County will work on documenting policies and procedures. The County will continue to work with the Auditor General's Office to adequately address our configuration management processes and potential risks to our resources.

Santa Cruz County
Corrective action plan
Year ended June 30, 2017

2017-05

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

Responsible officials' view: The County concurs with this finding

Name(s) of contact person(s): Robert Heming, Information Technology Director
Anticipated completion date: June 30, 2018

Corrective Action: The County will implement and test an off-site Disaster recovery solution that mirrors all systems in real time. Different disaster/risk IT scenarios will be developed and documented to address location-specific threats. The County is in the process of documenting the policies and procedures for contingency planning, staff training, and backup processes. The County will continue to work with the Auditor General's Office IT staff to adequately address our procedures regarding the contingency plan.

2017-06

The County Treasurer did not comply with state laws for apportioning interest earnings

Responsible officials' view: The County concurs with this finding

Name(s) of contact person(s): Liz Gutfahr, Treasurer
Anticipated completion date: June 30, 2019

Corrective Action: The County Treasurer's Office intends to change financial systems during fiscal year 2019. It is understood that the new system will allow the County Treasurer to apportion interest on a monthly or quarterly basis, as needed, for all investment accounts held by the Treasurer's Office.

Santa Cruz County
Corrective action plan
Year ended June 30, 2017

2017-07

The County should improve its policies and procedures for preparing its annual financial statements and note disclosures

Responsible officials' view: The County concurs with this finding

Name(s) of contact person(s): Mauricio A. Chavez, Administrative Services Director
Anticipated completion date: June 30, 2018

Corrective Action: The County will assign a staff member independent of the person preparing the financial statements to review the statements and related note disclosures. The County will continue to work with the Auditor General's Office and the independent consultant hired by the County to improve the accuracy of the financial statements.

Santa Cruz County
Corrective action plan
Year ended June 30, 2017

Federal Award Findings and Questioned Costs

2017-101

CFDA number and program name:	Not Applicable
Name(s) of contact person(s):	Mauricio A. Chavez, Administrative Services Director
Anticipated completion date:	June 30, 2018
Responsible officials' view:	The County concurs with this finding.

The County will develop and implement an effective review process when preparing the Schedule of Expenditures of Federal Awards. The County will work with an independent contractor to assist and ensure that policies and procedures are in place to capture all expenditures and potential subrecipients.

2017-102

CFDA number and program name:	97.067 Homeland Security Grant Program
Award numbers and years:	15-AZDOHS-HSGP-150406-02, October 1, 2015 through December 31, 2016; 15-AZDOHS-OPSG-150417-01, January 1, 2016 through December 31, 2016; 16-AZDOHS-HSGP-160405-01, October 1 2016 through September 30, 2017; 16-AZDOHS-OPSG-160420-01, November 1, 2016 through December 31, 2017
Name(s) of contact person(s):	Mauricio A. Chavez, Administrative Services Director
Anticipated completion date:	June 30, 2018
Responsible officials' view:	The County concurs with this finding.

The County made significant progress with the additional accountant focusing on fixed assets. The County performed an additional physical inventory in FY 2017 and was able to ensure that all equipment that was practical to tag was accomplished. The County hired an assistant to provide additional help to assure the County would comply with an effective control and accountability for all equipment and vehicles purchased with federal monies.

ADMINISTRATIVE SERVICES
SANTA CRUZ COUNTY

Mauricio A. Chavez, CMPI
Director of Finance &
Administrative Services

March 23, 2018

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*. 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,

Mauricio A. Chavez
Director of Finance & Administrative Services

2150 North Congress Drive | P.O. Box 1150 | Nogales, Arizona 85621
(520) 375-7820 | FAX (520) 375-7819 | TDD (520) 761-7816

Santa Cruz County
Summary schedule of prior audit findings
Year ended June 30, 2017

Status of financial statement findings

The County should improve its policies and procedures to accurately record and report financial information in its financial statements.

Finding number: 2016-01 & 2015-01
Status: Not corrected

The County was unable to correct this prior year finding due to a transition period at the County management level. The County will continue to work with the Auditor General's Office and the independent consultant to improve the accuracy of the financial statements.

The County Treasurer did not comply with state laws for apportioning interest income.

Finding number: 2016-02 & 2015-02
Status: Not corrected

The County Treasurer did not apportion interest due to timing constraints. The Treasurer anticipates implementing a new accounting system during fiscal year 2019, the County does not plan on implementing policies and procedures to apportion interest within the current system.

The County should improve access controls over its information technology resources.

Finding number: 2016-03 & 2015-03
Status: Not corrected

The County hired a new IT Director and will begin to implement the recommendations and work with the Auditor General's Office to address our access controls and potential risks to our information technology resources.

The County should improve its configuration management process over its information technology resources.

Finding number: 2016-04 & 2015-04
Status: Not corrected

The County hired a new IT Director and will begin to implement the recommendations and work with the Auditor General's Office to address our configuration management process and potential risks to our information technology resources.

Santa Cruz County
Summary schedule of prior audit findings
Year ended June 30, 2017

The County should improve its contingency planning procedures for its information technology resources.

Finding number: 2016-05
Status: Not corrected

The County hired a new IT Director and will begin to implement the recommendations and work with the Auditor General's Office to address our contingency planning procedures and potential risks to our information technology resources.

Status of federal award findings and questioned costs

CFDA number and program name: Not applicable
Finding number: 2016-101, 2015-101
Status: Not corrected

The County experienced a management transition process, and did not prepare an accurate and complete SEFA. New controls will be implemented to ensure a more accurate SEFA for the year ended June 30, 2018.

CFDA number and program name: 97.067 Homeland Security Grant Program
Finding number: 2016-102, 2015-102, 2014-102 & 2013-104
Status: Partially corrected

The County performed another physical inventory during FY 2017 and was able to account for and identify assets from the previous audit. The County was able to substantially improve the fixed assets listing including properly tagging equipment when practical.

CFDA number and program name: 93.268 Immunization Cooperate Agreement
Finding number: 2015-103
Status: Partially corrected

The County will implement and perform the required subrecipient monitoring procedures for fiscal year ended June 30, 2018.


ARIZONA
Auditor General
Making a Positive Difference