Financial Statement Findings and State Responses
(Reformatted from the FY 2016 Report on Internal Control and Compliance)

2016-01
The Arizona Department of Administration should prepare financial statements in a timely manner

Criteria: The Department of Administration (Department) should ensure the State's Comprehensive Annual Financial Report (CAFR) that includes its financial statements, note disclosures, required supplementary information, and other financial schedules is accurate and issued within the required timelines to satisfy the audit requirements imposed by federal and state laws and regulations, grants, contracts, and long-term debt agreements.

Condition and context: The Director of the Department is responsible for establishing and maintaining the State's accounting systems and preparing accurate and timely financial reports, including the State's CAFR. In accordance with Arizona Revised Statutes (A.R.S.) §41-703, the Director has the authority to promulgate rules, regulations, and procedures to carry out his responsibilities. Further, A.R.S. §35-131(I) requires state agencies and other organizations included in the State's reporting entity to submit all necessary financial statements and other required information to the Department to be used in preparing the State's CAFR. However, those statutes did not include provisions to enforce compliance, and as a result, state agencies did not always comply with the established deadlines. The Department had a November 2016 deadline to receive audited financial statements in order to issue the State's CAFR by December 31, 2016. Specifically, 14 state agencies had a November 2016 deadline to submit their audited financial statements; however, only 5 met this deadline. Further, the State's implementation of a new accounting system has contributed to the delay.

Effect: Since various state agencies did not submit all necessary financial statements and other required information to the Department in a timely manner, the Department was unable to prepare and issue the State's CAFR by its December 31, 2016, deadline. Delays in financial reporting may result in rating agencies lowering the State's ratings for bonds and certificates of participation. Also, the State's single audit reporting package will be issued late (see finding 2016-101), which could result in a loss of federal funding.

Cause: State statutes do not provide the Director of the Department with enforcement power to ensure that state agencies comply with department rules, regulations, and procedures for financial reporting. Further, the implementation of the new accounting system created delays in the Department preparing the State's CAFR and submitting it for audit.

Recommendation: To help ensure that the Department receives all financial information necessary to prepare and issue the State's CAFR in a timely manner, the Department should:

- Seek the authority to enforce rules, regulations, and procedures over financial reporting.
- Establish enforcement actions for agencies' failure to submit such information by the required deadlines.

This finding is similar to prior-year finding 2015-01 and is also reported as a federal finding. See finding 2016-101.

Agency Response: Concur

Agency: Department of Administration
Contact person: Clark Partridge, State Comptroller
Anticipated completion date: Unknown

Timeliness is still an issue. The FY16 State of Arizona Comprehensive Annual Financial Report (CAFR) was impeded due to delay in various agencies submitting their financial information and the implementation of the State's new accounting system. Arizona Revised Statutes (A.R.S.) §35-131 clearly requires State agencies and other organizations that are part of the State's reporting entity to submit all necessary financial information in accordance with the policies and procedures of the Arizona Department of Administration, General Accounting Office. This includes adherence to the established time frames and deadlines. However, there are no specific provisions in the law for actions that may be taken to enforce such compliance.

2016-02
The Department of Insurance should improve its workers' compensation claim management process over insolvent insurance carriers

Criteria: The Arizona Department of Insurance (Department) should have effective internal controls in place to ensure the workers' compensation claims and associated liabilities reported in the insurance department guaranty funds (guaranty funds) for insolvent insurance carriers are accurate and complete.

Condition and context: During fiscal year 2016, the Department used a third-party service organization to distribute approximately $12.1 million in insolvent insurance carriers' workers' compensation claims. Further, the service organization established the reserve balances that the Department used to estimate the guaranty funds' future liabilities. The June 30, 2016, liability was approximately $149 million. However, the Department did not establish adequate policies and procedures to ensure the claims paid and related reserve balances were accurate and complete. Specifically, the Department did not maintain adequate independent records to enable it to review and reconcile the claims and reserve balance data the service organization provided.

Effect: The Department could reimburse the service organization for invalid claimants or for inaccurate claim amounts. Further, the guaranty funds' estimated future liability may be misstated.

Cause: The Department received a monthly list of the insolvent insurance carriers' workers' compensation claims that the service organization processed and the reserve balances and reviewed the list to ensure that the detailed report totals agreed to the summary report totals. However, because of system limitations, the Department did not have records or controls to verify claimant information on the monthly lists were accurate and complete.

Recommendation: To help ensure the Department reimburses the service organization for the proper amounts and that estimated reserve balances are appropriate, the Department should establish independent records of workers' compensation claimant information and internal controls to reconcile those records to the data the service organization provided for accuracy and completeness.

Agency Response: Concur

The Department of Insurance (ADOI) the Arizona Property and Casualty Insurance Guaranty Fund (APCIGF) , which is organized within ADOI pursuant to A.R.S. 20-662(A) concur with the Auditor General's finding.

By way of background, the APCIGF became responsible for insolvent-insurer workers' compensation claims on June 1, 2015, when it assumed the responsibility from the Industrial Commission of Arizona. Since that time, the APCIGF Executive Director and Claims Manager recognized the need to migrate and store the workers' compensation claims data onto its own system but encountered barriers to implementation related to staffing resources, volume of claim files and computer upgrades required. The APCIGF and ADOI will expedite this effort in order to address this claim management process financial statement finding.

Corrective action planned: In order to address this financial statement finding, the APCIGF and ADOI will take the following actions:

1. Arrange to have workers' compensation open claims data migrated onto the APCIGF claim database. The ADOI will work with Lightspeed Data Systems, APCIGF's claims software vendor, to migrate the workers' compensation open claims data to the APCIGF's claims database.
2. As new workers' compensation claims are opened, claims will be created on the APCIGF database.
APCIGF will implement a process for obtaining and storing new claim data it obtains from the National Conference of Insurance Guaranty Funds' database or from insolvent insurer databases as appropriate.
3. APCIGF will implement a process to routinely update its own workers' compensation claims database in order to verify accuracy of claim payment amounts and recipients with respect to claims handled by APCIGF's contracted third party claim administrator.
4. APCIGF staff will upload claims data into the APCIGF database, and will upload claim file documents in an electronic document management system hosted by ICM Document Solutions. APCIGF will index documents uploaded to ICM with unique identifiers and other attributes that will connect each document
to the corresponding claims data in the APCIGF database, and that will facilitate document location and records management.
5. In order to implement the foregoing steps, the ADOI may need to upgrade APCIGF's server. Any upgrades necessary will be accomplished by September 30, 2017.

Despite the complexities involved, APCIGF and ADOI recognize the need to and importance of having workers' compensation claims data available in our claims database, and to implement a process that improves internal controls over claim payments. We are committed toward promptly accomplishing that goal.

2016-03
State agencies should improve their risk-assessment process to include information technology security

Criteria—The State faces risks of reporting inaccurate financial information and exposing sensitive data. An effective internal control system for the State's agencies should include an agency-wide risk-assessment process that involves members of an agency's administration and IT management to determine the risks an agency 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—Auditors reviewed the information technology security risk-assessment process at four state agencies including the Department of Economic Security (DES), Department of Revenue (DOR), Department of Child Safety (DCS), and Department of Administration (DOA). We determined that these agencies' annual risk-assessment processes did not include an agency-wide information technology (IT) security risk assessment over their IT resources, which include their systems, networks, infrastructure, and data. Also, these agencies did not identify and classify sensitive information. Further, these agencies did not evaluate the impact disasters or other system interruptions could have on their critical IT resources.

Effect—There is an increased risk that these agencies' administrators and IT management may not effectively identify, analyze, and respond to risks that may impact their IT resources.

Cause—These agencies lacked sufficient policies and procedures and detailed instructions for employees to follow.

Recommendations—To help ensure these agencies have effective policies and procedures to identify, analyze, and respond to risks that may impact their IT resources, these agencies need to implement an agency-wide IT risk-assessment process. The information below provides guidance and best practices to help these agencies 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. (DOA, DES, DOR)
- 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. (DOA, DES, DOR)
- 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's results should be considered when updating its disaster recovery plan. (DES, DOR)

This finding is similar to prior-year finding 2015-03 and 2015-09.

Agency Response: Concur

Agency: Department of Administration
Name of contact person and title: Clark Partridge, State Comptroller
Anticipated completion date: August 31, 2017

The State is aggressively working to correct all issues related to the access of its IT resources. State-wide risk-assessment processes will be expanded to include IT security. Each agency has developed a detailed corrective action plan to address this finding.

2016-04
State agencies should improve access controls over their information technology resources

Criteria—Logical and physical access controls help to protect a state agency'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, an agency should have effective internal control policies and procedures to control access to its IT resources.

Condition and context— Auditors reviewed access controls over information technology resources at four state agencies including the Department of Administration (DOA), Department of Economic Security (DES), Department of Revenue (DOR), and Department of Child Safety (DCS). We determined that these agencies did not have adequate policies and procedures or consistently implement their policies and procedures to help prevent or detect unauthorized or inappropriate access to their IT resources.

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

Cause—These agencies lacked sufficient policies and procedures and detailed instructions for employees to follow.

Recommendations—To help prevent and detect unauthorized access or use, manipulation, damage, or loss to these agencies' IT resources, these agencies need to develop and implement effective logical and physical access policies and procedures over their IT resources. The information below provides guidance and best practices to help these agencies 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. (DOA, DES, DCS, DOR)
• Remove terminated employees' access to its IT resources—Employees' network and system access should immediately be removed upon their terminations. (DOA, DES, DOR)
• 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. (DOA, DES, DCS, DOR)
• Review all shared accounts—Shared network access accounts should be reviewed and eliminated orminimized when possible. (DOA, DES, DOR)
• 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. (DOA, DES, DCS, DOR)
• Review and monitor key activity of users—Key activities of users and those with elevated access should be reviewed for propriety. (DOA, DES, DCS, DOR)
• Improve network and system password policies—Network and system password policies should be improved and ensure they address all accounts. (DOA, DES, DCS, DOR)
• 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. (DOA, DES)
• 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. (DOA, DES)
• 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. (DOA, DES)

This finding is similar to prior-year finding 2015-02, 2015-04 and 2015-08.

Agency Response: Concur

Agency: Department of Administration
Name of contact person and title: Clark Partridge, State Comptroller
Anticipated completion date: Unknown

The State is aggressively working to correct all issues related to the access of its IT resources. IT systems access is of the upmost importance to the State. Policy and procedures have been developed or are being developed to address any gaps and assure only appropriate access is granted to accounts. Each agency has developed a detailed corrective action plan to address this finding.

2016-05
State agencies should improve their configuration management processes over their information technology resources

Criteria—A well-defined configuration management process, including a change management process, is needed to ensure that a state agency'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. An agency should have effective written configuration management internal control policies and procedures to track and document changes made to its IT resources.

Condition and context—Auditors reviewed the information technology configuration management processes at four state agencies including the Department of Administration (DOA), Department of Economic Security (DES), Department of Revenue (DOR), and Department of Child Safety (DCS). We determined that these agencies' have written policies and procedures for managing changes to their IT resources; however, they lacked critical elements. Also, these agencies did not have policies and procedures to ensure IT resources were configured securely.

Effect—There is an increased risk that these agencies' 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—These agencies lacked sufficient policies and procedures and detailed instructions for employees to follow.

Recommendations—To help prevent and detect unauthorized, inappropriate, and unintended changes to these agencies' IT resources, these agencies need to update their policies and procedures over their configuration management processes. The information below provides guidance and best practices to help these agencies 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. (DOA, DES, DCS, DOR)
- Review proposed changes—Proposed changes to IT resources should be reviewed for appropriateness and justification, including consideration of the changes' security impact. (DOA, DOR)
- 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. (DOA, DOR)
- Roll back changes—Rollback procedures should be established that include documentation necessary to back out changes that negatively impact IT resources. (DOA, DES, DCS, DOR)
- Test—Changes should be tested prior to implementation, including performing a security impact analysis of the change. (DOA, DOR)
- 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. (DOA, DOR)
- Configure IT resources appropriately and securely—The functionality of IT resources should be limited to ensure it is performing only essential services and maintaining appropriate and secure configurations for all systems. (DOA, DES, DCS, DOR)
- 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. (DES, DCS, DOR)

This finding is similar to prior-year finding 2015-03 and 2015-09.

Agency Response: Concur

Agency: Department of Administration
Name of contact person and title: Clark Partridge, State Comptroller
Anticipated completion date: July 31, 2017

The State is aggressively working to correct all issues related to the access of its IT resources. Policy and procedures have been developed or are being developed to address any gaps in the States' IT configuration management processes. Each agency has developed a detailed corrective action plan to address this finding.

2016-06
State agencies should improve security over their information technology resources

Criteria—The selection and implementation of security controls for a state agency's information technology (IT) resources, which include its systems, network, infrastructure, and data, are important because they reduce the risks that arise from losing confidentiality, integrity, or availability of information that could adversely impact the agency's operations or assets. Therefore, an agency 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— Auditors reviewed the security controls over information technology resources at four state agencies including the Department of Administration (DOA), Department of Economic Security (DES), Department of Revenue (DOR), and Department of Child Safety (DCS). We determined that these agencies did not have sufficient written IT security policies and procedures over their IT resources.

Effect—There is an increased risk that these agencies may not prevent or detect the loss of confidentiality, integrity, or availability of systems and data.

Cause—These agencies lacked sufficient policies and procedures and detailed instructions for employees to follow.

Recommendations—To help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to these agencies' IT resources, these agencies need to further develop their policies and procedures over IT security. The information below provides guidance and best practices to help these agencies 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. (DOA, DES, DOR)
- 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. (DES, DOR)
- 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. (DOA, DES, DOR)
- 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. (DOA, DES, DOR)

• Apply patches—Patches to IT resources should be evaluated, tested, and applied in a timely manner once the vendor makes them available. (DOA, DES, DOR)
• Secure unsupported software—Establish a strategy for assessing and securing any software that the manufacturer no longer updates and supports. (DES)
• 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. (DOA, DES)
• 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 vendor's performance should be monitored to ensure conformance with vendor contracts. (DOA, DES, DOR)
• Implement IT standards and best practices—IT policies and procedures should be reviewed against current IT standards and best practices, updated where needed, and implemented entity-wide, as appropriate. Further, staff should be trained on IT policies and procedures. (DES)

This finding is similar to prior-year finding 2015-02, 2015-03, and 2015-09.

Agency Response: Concur

Agency: Department of Administration
Name of contact person and title: Clark Partridge, State Comptroller
Anticipated completion date: Unknown

The State is aggressively working to correct all issues related to the access of its IT resources. Policy and procedures have been developed or are being developed to address any lingering gaps related to IT security. Each agency has developed a detailed corrective action plan to address this finding.

2016-07
State agencies should improve their contingency planning procedures for their information technology resources

Criteria—It is critical that the State's agencies 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 an agency's 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 the plan's activation; and having system and data backup policies and procedures.

Condition and context—Auditors reviewed the contingency planning procedures at four state agencies including the Department of Administration (DOA), Department of Economic Security (DES), Department of Revenue (DOR), and Department of Child Safety (DCS). We determined that these agencies' contingency plans lacked certain key elements related to restoring operations in the event of a disaster or other system interruption of their IT resources. Also, although these agencies were performing system and data backups, they 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 their IT resources.

Effect—These agencies risk 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— These agencies lacked sufficient policies and procedures and detailed instructions for employees to follow.

Recommendations—To help ensure these agencies' operations continue in the event of a disaster, system or equipment failure, or other interruption, these agencies need to further develop their contingency-planning procedures. The information below provides guidance and best practices to help these agencies 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. (DOA, DES, DOR)

• 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. (DOA, DES, DOR)

• Test the contingency plan—A process should be developed and documented to perform regularly scheduled tests of the contingency plan and document the tests performed and results. This process should include updating and testing the contingency plan at least annually or as changes necessitate, and coordinating testing with other plans of the entity such as its continuity of operations, cyber incident response, and emergency response plans. Plan testing may include actual tests, simulations, or table top discussions and should be comprehensive enough to evaluate whether the plan can be successfully carried out. The test results should be used to update or change the plan. (DOA, DES, DOR)

• 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. (DOA, DES, DOR)

• 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. (DOA, DES, DOR)

This finding is similar to prior-year finding 2015-11.

Agency Response: Concur

Agency: Department of Administration
Name of contact person and title: Clark Partridge, State Comptroller
Anticipated completion date: Unknown

The State corrected some of these issues and continues to pursue appropriate corrective actions on the remaining gaps. Each agency has developed a detailed corrective action plan to address this finding.

2016-08
The Arizona Department of Administration's Data Center should strengthen their contracts with state agencies

Criteria—Information technology (IT) service contracts between the Arizona Department of Administration's Data Center (Data Center) and other state agencies should be complete, up to date, and include all parties' responsibilities. Well-documented and up-to-date service contracts provide staff with repeatable processes and clear expectations. In addition, the Data Center should maintain a comprehensive listing of state agencies it has provided services to and the services provided.

Condition and context—The Data Center's IT service contracts with state agencies are broad, not agency specific, and do not adequately address critical services, including disaster recovery. Consequently, agencies may not understand their responsibilities in the event of a disaster, including what they would need to provide (e.g., data, software, etc.) to the Data Center.

Effect—Current contracts for services between the Data Center and state agencies could result in the failure to clearly communicate policies and procedures, limit staff accountability, and result in inconsistencies. For example, if a major disruption or disaster were to occur, the order in which systems were restored may not match individual state agencies' or the State's criticality or operational priorities. In addition, state agencies might incorrectly assume that the Data Center will always provide full off-site backup and disaster recovery.

Cause—The Data Center did not have sufficient policies and procedures to help ensure their contracts with state agencies, including disaster recovery services, are specific for each state agency and are updated as needed. In addition, the Data Center did not maintain a comprehensive listing of state agencies it provided services to along with the services provided.

Recommendations—To help ensure IT service contracts between the Data Center and state agencies are complete and up to date, the Data Center should strengthen its IT services policies and procedures. The procedures should include establishing a comprehensive listing of the state agencies' systems maintained and clarifying the specific roles and responsibilities that all parties play in disaster recovery efforts. Further, the Data Center should ensure that the services provided are appropriately identified on the listing, state agency systems are prioritized for recovery based on their relative importance, and the listing is updated as the needs of the state agency changes. The information from the listing should also be included in the IT service contract with each state agency and provided either in summary form or a contract revision to each state agency.

This finding is similar to prior-year finding 2015-05.

Agency Response: Concur

Agency: Department of Administration
Name of contact person and title: Gary Hensley, Chief Operating Officer
Anticipated completion date: February 1, 2017

ADOA has developed agency specific language within our inter-agency agreements for the specific services we deliver and what specific services we do not deliver, to include disaster recovery, for each agency. We have also worked with the agencies to get them executed. This was fully implemented February 1, 2017.

2016-09
The Department of Administration's State Procurement Office should strengthen its policies and procedures over monitoring its contract with its ProcureAZ vendor

Criteria— The Department of Administration's State Procurement Office (SPO) contracted with a vendor to support and host the State's procurement system (ProcureAZ). This vendor also used a subcontractor to perform some of these services for the ProcureAZ system. Accordingly, the SPO should monitor the contract to ensure the vendor and its subcontractor met the terms and conditions.

Condition and context— Based on review of the contract and the applicable amendments, auditors noted there were several deficiencies related to SPO ensuring the contractor and its subcontractor adhered to the contract requirements over the ProcureAZ system, as follows:

- The contract provided for the State to perform an audit or inspection of the vendor records as they relate to the ProcureAZ system; however, the SPO did not monitor the vendor's internal controls or require that a service organization internal control audit in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16, Type II, be performed and submitted to the SPO.
- The contract required the vendor to demonstrate, at least once a year, the successful recovery of the ProcureAZ system should a disaster occur; however, auditors determined the SPO did not obtain and review the results of the annual disaster recovery assessment from the vendor.
- The SPO was not always aware of all the terms and conditions in the contract. Specifically, auditors requested various reports from the SPO to list transactions that were created and approved by the same user, but the SPO was unable to generate the reports from the ProcureAZ system. These reports were included within the scope of the contract work, and therefore, SPO should have generated and reviewed these reports during the year.

• The contract included service levels agreements (SLAs) that the vendor should meet. However, the SPO did not have a process in place to track and monitor these results to ensure the service levels were being met. As such, auditors were unable to determine if the vendor complied with this requirement.
Effect: Federal grant monies were awarded to a subrecipient by a member of department management when a conflict of interest existed in violation of state personnel rules, A.R.S. §38-501 et seq., and 2 CFR §200.317. Further, auditors found evidence that improper payments and abuse had occurred in relation to the monies awarded and expended by the JTED. In addition, this finding could potentially affect other federal programs that the Department administered.

Effect—The SPO may not be able to ensure the vendor and its subcontractor are fulfilling their contract responsibilities or obtain the necessary information or data and assurances that the vendor's system of internal controls are operating effectively.

Cause—The SPO did not have written policies and procedures to monitor and ensure the vendor and its subcontractor met all requirements set forth in the contract. In addition, throughout the contract period there was turnover with the personnel responsible for overseeing the contract.

Recommendations— The SPO should develop and implement comprehensive procurement policies and procedures to help ensure that it monitors its vendor and subcontractor compliance with the terms and conditions of the ProcureAZ contract.

Agency's Response: Concur

Agency: Department of Administration
Name of contact person and title: Ashoke Seth, State Procurement Officer
Anticipated completion date: Unknown

The State will evaluate and address any gaps that are related to the State's procurement system for current and future implementation.

2016-10
The Department of Revenue should continue to strengthen its procedures for processing income tax revenues

Criteria: The Department of Revenue (Department) should improve procedures to ensure that it collects and reports all state income taxes.

Condition and context: The Department is responsible for collecting and reporting state income taxes. While testing the Department's procedures for collecting and reporting state income tax revenues, auditors noted additional procedures that the Department should perform to help ensure all state income taxes are collected and reported. Certain information has been omitted from this finding because of its sensitive nature. Therefore, specific details, including detailed recommendations, were verbally communicated to those officials directly responsible for implementing corrective action.

Effect: The State may not receive the proper amount of income taxes.

Cause: The Department's information system did not have the functionality to perform the identified omitted procedures.

Recommendation: The Department should implement additional procedures necessary to compensate for the omitted procedures.

This finding is similar to prior-year finding 2015-10.

Agency Response: Concur

Agency: Department of Revenue
Name of contact person and title: Francis Becker, Senior Internal Auditor
Anticipated completion date: Unknown

The Department of Revenue will continue to expand its manual procedures over this process. To fully remediate this finding however, the Department must expand its current IT functionality over this process, which will require additional funding that is not currently

available. The Department is continually implementing manual procedures to mitigate the associated risks and is currently researching automation tools that would efficiently and effectively remediate any remaining deficiencies over this process.