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

2017-01
The four state agencies named below 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—The information technology security risk-assessment process was reviewed at four state agencies including the Department of Administration (DOA), Department of Economic Security (DES), Department of Child Safety (DCS), and Department of Revenue (DOR). The DES is partially responsible for the DCS' controls over its risk assessment process. 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 develop and implement an effective 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, DCS, 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, DCS, 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)

The State'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.

Agency Response: Concur

Agency: Department of Administration
Contact person: Clark Partridge, State Comptroller, (602-542-5405)
Anticipated completion date: Unknown

The State is actively 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.

2017-02
The four state agencies named below 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 access. Therefore, an agency should have effective internal control policies and procedures to control access to its IT resources.

Condition and context—Access controls over information technology resources were reviewed at four state agencies including the Department of Administration (DOA), Department of Economic Security (DES), Department of Child Safety (DCS), and Department of Revenue (DOR). The DES is partially responsible for DCS' access controls. 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 effective logical and physical access policies and procedures over their IT resources. These agencies should review their policies and procedures against current IT standards and best practices and implement them agency-wide, as appropriate. Further, these agencies should train staff on the policies and procedures. 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 or minimized 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. (DES, 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, 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, DOR)
- 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, DOR)
- 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, DOR)
- Data sharing—Data-sharing agreements should be sufficiently designed to include data security restrictions for confidential information, and these agreements should be monitored. (DOR)

The State'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.

Agency Response: Concur

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

The State is actively working to correct all issues related to the access of its IT resources. IT systems assess 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.

2016-03
The four state agencies named below 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—The information technology configuration management processes were reviewed at four state agencies including the Department of Administration (DOA), Department of Economic Security (DES), Department of Child Safety (DCS), and Department of Revenue (DOR). The DES is partially responsible for the DCS' controls over its configuration management processes. These agencies have written policies and procedures for managing changes to their IT resources; however, some of these agencies lacked critical elements, and the agencies did not consistently implement their configuration management policies and procedures. 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 review their configuration management policies and procedures against current IT standards and best practices, update them where needed, and implement them agency-wide, as appropriate. Further, these agencies should train staff on the policies and procedures. 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, 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, 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 postimplementation review of the change to confirm the change followed the change management process and was implemented as approved. (DOR)
• **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. (DOA, DES, 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, DOR)

The State'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.

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 actively 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.

2017-04
The four state agencies named below 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—The security controls over information technology resources were reviewed 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). The DES is partially responsible for the DCS' controls over information technology security. 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. These agencies should review their policies and procedures against current IT standards and best practices and implement them agency-wide, as appropriate. Further, the agencies should train staff on the policies and procedures. 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 the entity's other departments 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, DOR)

• **Develop and document a process for awarding IT vendor contracts—**A process should be developed and documented to ensure the consideration of IT risks, costs, benefits, and technical specifications prior to awarding IT vendor contracts. In addition, contracts should include specifications addressing the management, reliability, governance, and security of the entity's IT resources. Further, for cloud services, ensure service contracts address all necessary security requirements based on best practices, such as physical location of data centers. Finally, IT vendors' performance should be monitored to ensure conformance with vendor contracts. (DOA, DES)

The State'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 2016-06.

Agency Response: Concur

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

The State is actively 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.

2017-05
The four state agencies named below 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—The contingency planning procedures were reviewed 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). The DES is responsible for all the DCS' controls over contingency planning. 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. These agencies should review their contingency planning procedures against current IT standards and best practices, update them where needed, and implement them agency-wide, as appropriate. 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)
- 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. (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. (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 the entity's other plans such as its continuity of operations, cyber incident response, and emergency response plans. Plan testing may include actual tests, simulations, or tabletop discussions and should be comprehensive enough to evaluate whether the plan can be successfully carried out. The test results should be used to update or change the plan. (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)

The State'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 2016-07.

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.

2017-06
The Department of Administration's Data Center should strengthen its contracts with state agencies

Criteria—Information technology (IT) service contracts between the 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 state agency's needs change. 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.

The State'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 2016-08.

Agency Response: Concur

Agency: Department of Administration
Name of contact person and title: Clark Partridge, State Comptroller

Anticipated completion date: Unknown

ADOA-ASET will work to delineate responsibilities between ADOA and state agency responsibilities and then strengthen contracts.

2017-07
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 contract terms and conditions.

Condition and context—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 perform an internal control audit in accordance with Statement on Standards for Attestation Engagements No. 16, Type II, and submit the audit report 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, the SPO did not obtain and review the results of the annual disaster recovery assessment from the vendor.
• The contract included service level agreements that the vendor should meet. However, the SPO did not have a documented process in place to track and monitor these results to ensure the vendor was meeting the service levels. As such, the SPO did not determine if the vendor complied with this requirement.

Effect—The SPO did not ensure that the vendor and its subcontractor were fulfilling their contract responsibilities or obtain the necessary information or data and assurances that the vendor's system of internal controls is 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, and as a result there was no continuity of SPO staff to evaluate vendor and subcontractor compliance with 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.

The State'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 2016-09.

Agency Response: Concur

Agency: Department of Administration
Name of contact person and title: Mike Hladik, IT Procurement Manager
Anticipated completion date: March 31, 2019

Procedures and documentation for monitoring the ProcureAZ SLAs attached to the contract were implemented during the 2017 fiscal year. As part of the implementation of the new eprocurement system, SPO will clearly define roles and responsibilities for monitoring vendor performance to the contract, including who monitors performance to the SLAs and associated deliverables (such as any system and/or disaster recovery testing as included in the SLAs), and who monitors performance to contract terms and conditions outside of the SLAs and associated deliverables (such as any external audits and reporting). Ivalua provides for vendor performance events within the application to facilitate and track performance to contract terms.

2017-08
The Department of Education should reconcile its internal information system to the State's general ledger accounting system

Criteria—In accordance with the State of Arizona Accounting Manual (SAAM), Topic 05: Internal Controls, Section 05, General Internal Controls, 3, each agency must reconcile relevant activity not later than the end of the month following the month in which the transactions occurred and no less frequently than once a month. Further, reconciliations should be documented and retained in accordance with state record retention requirements.

Condition and context—During fiscal year 2017, the Department of Education (Department) distributed approximately $3.79 billion in basic state aid to school districts and charter schools and $442.5 million in classroom site fund monies to school districts and charter schools. The Department uses its own internal system to account for student count information and to calculate the amount of basic state aid and classroom site fund disbursements to the school districts and charter schools. However, the distribution amounts in its internal information system were not reconciled to the accounting records on the State's general ledger accounting system that was used to generate the payments to the school districts and charter schools. As a result, the Department was unable to readily provide explanations for significant variances between the two systems.

Effect—The Department was not in compliance with the SAAM and could have distributed inaccurate amounts to the school districts and charter schools. However, the Department subsequently performed the reconciliation and was able to explain the significant variances.

Cause—The Department did not have policies and procedures in place to perform a monthly reconciliation of its internal information system to the State's general ledger accounting system.

Recommendation—To help ensure the Department complies with the SAAM and amounts distributed to school districts and charter schools are accurate, the Department should develop policies and procedures to reconcile its internal information system to the State's general ledger accounting system for accuracy at least monthly. In addition, documentation of the reconciliation should be retained in accordance with state record retention requirements.

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

Agency Response: Concur

Agency: Department of Education
Name of contact person and title: Tammy Seilheimer, Chief Auditor
Anticipated completion date: December 2018

The Arizona Department of Education (ADE) agrees with this finding and will implement the recommendation. Each of the School Finance department's payment systems will be reconciled by the Fiscal Operations Director to system generated payment reports (where applicable) and the Arizona Financial Information System (AFIS) on a monthly basis, with each reconciliation being digitally saved. Apportionment (APOR) and Charter State Aid Apportionment (CHAR) do not have system generated reports for payment purposes. Reports submitted for payment are created with Access and Excel, while Classroom Site Fund (CSF) and Instructional Improvement Fund (IIF) systems generate detailed monthly payment reports. ADE's systems will be updated to facilitate the reconciliation process and ensure accuracy.

2017-09
The Department of Insurance should improve its workers' compensation claim management process over insolvent insurance carriers

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

Condition and context—During fiscal year 2017, the Department used a third-party service organization to distribute approximately $10.4 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, 2017, worker's compensation liability was approximately $143.7 million. Specifically, the Department did not maintain adequate independent records to enable it to review and reconcile the claims data the service organization provided.

Effect—The Department could reimburse the service organization for invalid claimants or for inaccurate claim amounts.

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 was accurate and complete.

Recommendation—To help ensure the Department reimburses the service organization for the proper amounts, 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.

The State'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.

Agency's Response: Concur

Agency: Department of Insurance
Name of contact person and title: Keith Schraad, Interim Director of Insurance
Scott Greenberg, Assistant Deputy Director
Michael Surguine, Guaranty Funds Executive Director
Anticipated completion date: December 31, 2018

The Department of Insurance (Department) concurs that the Department did not maintain adequate independent records to enable it to review and reconcile claims.

In addition to continuing to review payments issued by the administrator as presented on check registers,
• Effective January 1, 2018, the Department contracted with a third-party administrator that provides access to its claims system, so that Guaranty Fund staff will be able to monitor the status of all claims assigned to the third-party administrator. Further, Guaranty Fund staff will obtain a daily register of all payments made by the third-party administrator with respect to the assigned claims, so a reasonable sample of the payments may be tested for accuracy and propriety.
• By June 30, 2018, the Department will engage an auditor to perform a financial field audit on the claim administrator, which will include transaction testing, an internal controls evaluation of the administrator's policies and procedures, and an evaluation of whether the policies and procedures are consistently applied and followed.
• By August 31, 2018, the auditor will present the Department a report of its findings and opinion concerning the quality of the internal controls the administrator has in place, and the quality of the administrator's application of those controls.
• By September 30, 2018, the Department will confer with the administrator concerning any deficiencies the auditor found, and will expect the administrator to provide a plan to resolve the deficiencies by December 31, 2018.

2017-10
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 all of the State's income taxes. The Department's procedures for collecting and reporting income taxes were not sufficient to ensure all of the State's income taxes are collected and reported. Certain information in this finding has been omitted 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 additional procedures needed to help ensure all income taxes are collected and reported.

Recommendation—To help ensure the Department is collecting and reporting all of the State's income taxes, the Department should implement additional procedures necessary to compensate for the omitted procedures.

The State'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 2016-10.

Agency Response: Concur

Agency: Department of Revenue
Name of contact person and title: Nicole LaPella, Chief Internal Auditor
Anticipated completion date: Unknown

The Department of Revenue continues to explore various methodologies to strengthen its procedures for processing income tax revenues.

2017-11
The Department of Revenue should have effective policies and procedures in place to ensure unclaimed and abandoned tax refunds are reported to the Department's Unclaimed Property Unit and are properly reported in the State's financial statements

Criteria—The Department of Revenue (Department) should have effective internal control policies and procedures in place to ensure taxes receivable and unclaimed property reported in the State's financial statements are accurate and complete, and that it tracks and reports unclaimed and abandoned tax overpayments (refunds) to the Department's Unclaimed Property Unit, as required by state statutes.

Condition and context—The Department is responsible for collecting and reporting state income and sales taxes, including remitting taxpayer refunds in a timely manner. Further, the Department is responsible for submitting accurate and complete financial information to the Department of Administration to be used in preparing the State's comprehensive annual financial report. Taxes receivable recorded in the State's general fund is based on outstanding amounts due from taxpayers at fiscal year-end, net of allowances that include refunds owed to taxpayers. However, the Department was not complying with state statutes that require unclaimed and abandoned monies that include unclaimed and abandoned tax refunds be reported to the Department's Unclaimed Property Unit following the requirements of Arizona Revised Statutes §44- 302 A.11 and §44-307 A. In addition, unclaimed and abandoned tax refunds were still being included in the amounts deducted from the taxes receivable balance at fiscal year-end recorded on the State's financial statements, and the Department did not have procedures in place to identity such refunds and adjust the State's financial statements. Once these refunds become unclaimed or abandoned they should no longer be reported as an allowance to taxes receivable for financial reporting purposes. The Department provided an estimate of the misstatements to the Department of Administration, and the State's financial statements were adjusted for these errors.

Effect—In the preliminary draft of the general fund financial statements, taxes receivable and unavailable revenues were understated by $52.7 million, or by 1.5 percent of total assets and total liabilities and fund balance. Further, taxpayers may not be aware that they have unclaimed or abandoned tax refunds because these unclaimed and abandoned refunds had not been reported to the Department's Unclaimed Property Unit.

Cause—The Department did not have sufficient resources to develop appropriate policies and procedures to track and report unclaimed and abandoned tax refunds to the Department's Unclaimed Property Unit and properly report these tax refunds in the State's financial statements.

Recommendation—The Department should develop and implement policies and procedures necessary to identify, track, and report unclaimed and abandoned tax refunds to the Department's Unclaimed Property Unit and ensure that these refunds are properly reported in the State's financial statements. The State's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

Agency Response: Concur

Agency: Department of Revenue

Name of contact person and title: Nicole LaPella, Chief Internal Auditor
Anticipated completion date: Unknown

The Department of Revenue is looking into various solutions to take appropriate actions to remediate this finding and comply with Arizona Revised Statutes including updating and implementing policies and procedures to ensure unclaimed and abandoned tax refunds are reported to the Department's Unclaimed Property Unit.

2017-12
Northern Arizona University should improve its risk-assessment process over information technology security

Criteria—Northern Arizona University (University) 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 University's administration and information technology (IT) management to determine the risks the University 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 University's annual risk-assessment process did not include an adequate university-wide IT security risk assessment over the University's IT resources, which include its systems, network, infrastructure, and data. Also, the University did not have adequate policies and procedures to identify and classify sensitive information. Further, the University did not evaluate the impact disasters or other system interruptions could have on its critical IT resources and business operations.

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

Cause—The University had not reviewed its policies and procedures to ensure they were in line with current IT standards and best practices.

Recommendations—To help ensure the University has effective policies and procedures to identify, analyze, and respond to risks that may impact its IT resources, the University needs to improve its University wide IT risk-assessment process. The information below provides guidance and best practices to help the University achieve this objective:

• Conduct an IT risk-assessment process at least annually—A risk-assessment process should include the identification of risk scenarios, including the scenarios' likelihood and magnitude; documentation and dissemination of results; review by appropriate personnel; and prioritization of risks identified for remediation. An IT risk assessment could also incorporate any unremediated threats identified as part of an entity's security vulnerability scans.
• Identify, classify, inventory, and protect sensitive information—Security measures should be developed to identify, classify, and inventory sensitive information and protect it, such as implementing controls to prevent unauthorized access to that information. Policies and procedures should include the security categories into which information should be classified, as well as any state statutes and federal regulations that could apply, and require disclosure to affected parties if sensitive information covered by state statutes or federal regulations is compromised.
• Evaluate the impact disasters or other system interruptions could have on critical IT resources— The evaluation should identify key business processes and prioritize the resumption of these functions within time frames acceptable to the entity in the event of contingency plan activation. Further, the results of the evaluation should be considered when updating its disaster recovery plan.

Northern Arizona University's responsible officials' views and planned corrective action are in its corrective action plan included in the Universities Responses section at the end of this report. This finding was also reported in Northern Arizona University's separately issued report on internal control and compliance for the year ended June 30, 2017, as finding 2017-01.

Agency Response: Concur

Agency: Northern Arizona University
Name of contact person and title: Steve Burrell, Chief Information Officer
Anticipated completion date: December 31, 2018

To help ensure the university has adequate policies and procedures to identify, analyze, and respond to risks that may affect IT resources, the university will improve its university-wide IT risk-assessment process and align it with NIST best practices.

2017-13
Northern Arizona University should improve access controls over its information technology resources

Criteria—Logical access controls help to protect Northern Arizona University's (University) 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 University should have effective internal control policies and procedures to control access to its IT resources.

Condition and context—The University 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 University 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 University had not reviewed its policies and procedures to ensure they were in line with current IT standards and best practices.

Recommendations—To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the University needs to develop and implement effective logical access policies and procedures over its IT resources. The University should review these policies and procedures against current IT standards and best practices and implement them university-wide, as appropriate. Further, the University should train staff on the policies and procedures. The information below provides guidance and best practices to help the University 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.
- 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.
- Manage employee-owned electronic devices connecting to the network—The use of employee-owned electronic devices connecting to the network should be managed, including specifying configuration requirements and the data appropriate to access; inventorying devices; 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.

Northern Arizona University's responsible officials' views and planned corrective action are in its corrective action plan included in the Universities Responses section at the end of this report. This finding was also reported in Northern Arizona University's separately issued report on internal control and on compliance for the year ended June 30, 2017, as finding 2017-02.

Agency Response: Concur

Agency: Northern Arizona University
Name of contact person and title: Steve Burrell, Chief Information Officer
Anticipated completion date: December 31, 2018

To help prevent and detect unauthorized access or use, manipulation, damage, or loss to IT resources, the university will implement effective logical access policies and procedures over its IT resources in alignment with NIST best practices and train faculty and staff

on those policies and procedures. The university will utilize the NIST framework to continue enhancing existing access request policy and procedures for enterprise systems.

2017-14
Northern Arizona University 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 Northern Arizona University's (University) 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 University 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 University has written policies and procedures for managing changes to its IT resources; however, they were not fully implemented as of fiscal year-end. Also, the University did not have policies and procedures to ensure all IT resources were configured securely.

Effect—There is an increased risk that the University'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 University made significant changes to its configuration management policies and procedures but had not fully implemented all of these changes as of fiscal year-end. Further, the University had not reviewed all of its policies and procedures to ensure they were in line with current IT standards and best practices.

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

• Establish and follow change management processes—For changes to IT resources, a change management process should be established for each type of change, including emergency changes and other changes that might not follow the normal change management process. Further, all changes should follow the applicable change management process and should be appropriately documented.
• Review proposed changes—Proposed changes to IT resources should be reviewed for appropriateness and justification, including consideration of the change's security impact.
• Document changes—Changes made to IT resources should be logged and documented, and a record should be retained of all change details, including a description of the change, the departments and system(s) impacted, the individual responsible for making the change, test procedures performed and the test results, security impact analysis results, change approvals at each appropriate phase of the change management process, and a post-change review.
• Roll back changes—Roll-back 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 postimplementation 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.

Northern Arizona University's responsible officials' views and planned corrective action are in its corrective action plan included in the Universities Responses section at the end of this report. This finding was also reported in Northern Arizona University's separately issued report on internal control and on compliance for the year ended June 30, 2017, as finding 2017-03.

Agency Response: Concur

Agency: Northern Arizona University
Name of contact person and title: Steve Burrell, Chief Information Officer
Anticipated completion date: December 31, 2018

To help prevent and detect unauthorized, inappropriate, and unintended changes to IT resources, the university will implement effective configuration management policies and procedures over its IT resources in alignment with NIST best practices and train faculty and staff on those policies and procedures. The university will continue to enhance existing change management and configuration policy and procedures.

2017-15
Northern Arizona University should improve security over its information technology resources

Criteria—The selection and implementation of security controls for Northern Arizona University's (University) 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 University's operations or assets. Therefore, the University 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 University did not have sufficient written IT security policies and procedures over its IT resources.

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

Cause—The University had not reviewed its policies and procedures to ensure they were in line with current IT standards and best practices.

Recommendations—To help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources, the University needs to further develop its IT security policies and procedures. The University should review these policies and procedures against current IT standards and best practices and implement them university-wide, as appropriate. Further, the University should train staff on the policies and procedures. The information below provides guidance and best practices to help the University 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 insider threats. Security awareness training should be provided to new employees and on an ongoing basis.

• Document IT vulnerability scans policies and procedures—Policies and procedures should address the formal process for 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, policies and procedures should require that vulnerability scan reports and results be analyzed and legitimate vulnerabilities remediated as appropriate, and information obtained from the vulnerability-scanning process should be shared with the entity's other departments to help eliminate similar vulnerabilities.
• Apply patches—Patches to IT resources should be evaluated, tested, and applied in a timely manner once the vendor makes them available.
• 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.

Northern Arizona University's responsible officials' views and planned corrective action are in its corrective action plan included in the Universities Responses section at the end of this report. This finding was also reported in Northern Arizona University's separately issued report on internal control and on compliance for the year ended June 30, 2017, as finding 2017-04.

Agency Response: Concur

Agency: Northern Arizona University
Name of contact person and title: Steve Burrell, Chief Information Officer
Anticipated completion date: December 31, 2018

Policies and procedures that align with NIST best practices and standards are being drafted by the university to improve security over its information technology resources. Existing policies and procedures will continue being enhanced to align with the latest NIST best practices and guidelines.

2017-16
Northern Arizona University should improve its contingency planning procedures for its information technology resources

Criteria—It is critical that Northern Arizona University (University) 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 University's contingency plan lacked certain key elements related to restoring operations in the event of a disaster or other system interruption of its IT resources. Also, although the University 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 University 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 University had not reviewed its policies and procedures to ensure they were in line with current IT standards and best practices. Additionally, the University had not updated its incident management plan based on the results of its most recent test of the plan.

Recommendations—To help ensure university operations continue in the event of a disaster, system or equipment failure, or other interruption, the University needs to further develop its contingency planning procedures. The University should review its contingency planning procedures against current IT standards and best practices, update them where needed, and implement them university-wide, as appropriate. The information below provides guidance and best practices to help the University 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.
• Test the contingency plan—A process should be developed and documented to perform regularly scheduled tests of the contingency plan and document the tests performed and results. This process should include updating and testing the contingency plan at least annually or as changes necessitate, and coordinating testing with the entity's other plans such as its continuity of operations, cyber incident response, and emergency response plans. Plan testing may include actual tests, simulations, or tabletop discussions and should be comprehensive enough to evaluate whether the plan can be successfully carried out. The test results should be used to update or change the plan.
• 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. Northern Arizona University's responsible officials' views and planned corrective action are in its corrective action plan included in the Universities Responses section at the end of this report. This finding was also reported in Northern Arizona University's separately issued report on internal control and on compliance for the year ended June 30, 2017, as finding 2017-05.

Agency Response: Concur

Agency: Northern Arizona University
Name of contact person and title: Steve Burrell, Chief Information Officer
Anticipated completion date: December 31, 2018

To help ensure its operations continue in the event of a disaster, system or equipment failure, or other interruption, the university will further enhance its current contingency planning procedures in alignment with NIST best practices.

2017-17
The University of Arizona should strengthen oversight of its information technology internal controls

Criteria—A strong control environment should include a governance structure that provides oversight and requires policies and procedures that are documented, communicated to employees, and consistently applied. In addition, an effective internal control system should include monitoring of internal controls to ensure that employees are following the University of Arizona's (University) policies and procedures.

Condition and context—The University had policies and procedures over most of its information technology (IT) resources, which include its systems, network, infrastructure, and data. However, the University did not monitor its policies and procedures over its IT resources to ensure that they were established and followed.

Effect—There is an increased risk that the University may not achieve its internal control objectives as they relate to IT security and integrity.
Cause—The University is a complex system of colleges and business units, each with their own IT personnel and IT resources. Although the University centralized some aspects of IT internal controls, it had not clearly designated oversight and monitoring responsibilities for those IT internal controls that were not centralized.

Recommendations—To help ensure that the University maintains a strong control environment and effective internal controls over its IT resources, the University should clearly designate oversight and perform monitoring over its IT internal controls to help ensure that they are in place and followed.

The University of Arizona's responsible officials' views and planned corrective action are in its corrective action plan included in the Universities Responses section at the end of this report. This finding was also reported in the University of Arizona's separately issued report on internal control and on compliance for the year ended June 30, 2017 as finding 2017-01.

Agency Response: Concur

Agency: University of Arizona
Name of contact person and title: Lanita Collete, Chief Information Officer
Anticipated completion date: May 2018

The University acknowledges that oversight of technical controls in our distributed computing environment needs improvement. To address this need, UA leadership appointed a Chief Information Security Officer to build a University security program, who will work with campus leadership to facilitate decentralized IT units' adherence to University IT policy. As part of this program, we are deploying monitoring tools on the UA network that can be leveraged by both central and distributed staff. We also will produce and distribute "playbooks" to assist distributed staff to appropriately and consistently handle security incidents.

2017-18
The University of Arizona should improve its risk-assessment process over information technology security

Criteria—The University of Arizona (University) 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 University's administration and information technology (IT) management to determine the risks the University 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 University did not complete its risk-assessment process over its IT resources, which include its systems, network, infrastructure, and data. Also, the University did not always follow its policies to identify and classify sensitive information. Further, the University 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 University's administration and IT management may not effectively identify, analyze, and respond to risks that may impact its IT resources.

Cause—The University developed policies and procedures addressing risk-assessment and data classification but did not have a process in place to ensure they were fully implemented. Additionally, a business impact analysis had not been performed.

Recommendations—To help ensure the University has effective policies and procedures to identify, analyze, and respond to risks that may impact its IT resources, it needs to fully implement its IT risk assessment process. The information below provides guidance and best practices to help the University achieve this objective:

• Complete an IT risk-assessment process in accordance with its policies and procedures—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.
• Implement its policies and procedures for identifying, classifying, inventorying, and protecting sensitive information—Security measures should be implemented to identify, classify, and inventory sensitive information and protect it, such as implementing controls to prevent unauthorized access to that information in accordance with the University's data classification and handling standard.
• 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 University in the event of contingency plan activation. Further, the results of the evaluation should be considered when updating its disaster recovery plan.

The University of Arizona's responsible officials' views and planned corrective action are in its corrective action plan included in the Universities Responses section at the end of this report. This finding was also reported in the University of Arizona's separately issued report on internal control and on compliance for the year ended June 30, 2017, as finding 2017-02.

Agency Response: Concur

Agency: University of Arizona

Name of contact person and title: Lanita Collete, Chief Information Officer
Anticipated completion date: May 2018

The University acknowledges that our IT risk assessment process needs additional work. To supplement our current product-specific risk assessments and our annual self-assessment process, we will engage professional services for comprehensive assessments mapped to appropriate compliance standards. We will then begin work on prioritized recommendations from the assessments, including identifying and classifying sensitive information. We will also conduct an evaluation of our disaster recovery plan to ensure that key business needs are prioritized and adequately addressed.

2017-19
The University of Arizona should improve access controls over its information technology resources

Criteria—Logical access controls help to protect the University of Arizona's (University) information technology (IT) resources, which include its enterprise 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 University should have effective internal control policies and procedures to control access to its IT resources.

Condition and context—The University did not have adequate policies and procedures for logging and monitoring users with elevated access within its enterprise systems.

Effect—There is an increased risk that the University 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 University had not established written policies and procedures for logging and monitoring users with elevated access within its enterprise systems. The University was aware that technology is available to assist with this process, but the University is not currently utilizing any of these tools.

Recommendations—To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the University needs to develop and implement effective logical access policies and procedures for logging and monitoring users with elevated access within its enterprise systems. In addition, key activities of users with elevated access should be reviewed regularly for propriety. The University should review these policies and procedures against current IT standards and best practices. Further, the University should train staff on the policies and procedures.

The University of Arizona's responsible officials' views and planned corrective action are in its corrective action plan included in the Universities Responses section at the end of this report. This finding was also reported in the University of Arizona's separately issued report on internal control and on compliance for the year ended June 30, 2017, as finding 2017-03.

Agency Response: Concur

Agency: University of Arizona
Name of contact person and title: Lanita Collete, Chief Information Officer
Anticipated completion date: December 2018

The University acknowledges a lack of logging and monitoring of elevated access to enterprise systems and will move forward to develop and implement effective logical access policies and procedures.

2017-20
The University of Arizona should improve security over its information technology resources

Criteria—The selection and implementation of security controls for the University of Arizona's (University) information technology (IT) resources, which include its enterprise 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 University's operations or assets. Therefore, the University should further develop and fully implement internal control policies and procedures for an effective IT security process that include practices to help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources.

Condition and context—The University did not fully implement its existing IT security policies and procedures, and in some cases did not have sufficient written security policies and procedures over its IT resources.
Effect—There is an increased risk that the University may not prevent or detect the loss of confidentiality, integrity, or availability of data and systems.
Cause—The University developed some policies and procedures for IT security but did not have a process in place to ensure they were fully implemented and lacked detailed policies and procedures for some IT security areas.

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 University needs to further develop its policies and procedures over IT security. The University should review these policies and procedures against current IT standards and best practices and implement them university-wide, as appropriate. Further, the University should train staff on the policies and procedures. The information below provides guidance and best practices to help the University achieve this objective:

• Improve its incident response plan—The incident response plan should be further developed 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. All security incidents should be reported to incident response personnel so they can be tracked and documented. Policies and procedures should also follow regulatory and statutory requirements and require making disclosures to affected individuals and appropriate authorities if an incident occurs.
• 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 to help eliminate similar vulnerabilities.
• Protect sensitive or restricted data—Restrict access to media containing data the University, 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 University's data classification and handling standard.

The University of Arizona's responsible officials' views and planned corrective action are in its corrective action plan included in the Universities Responses section at the end of this report. This finding was also reported in the University of Arizona's separately issued report on internal control and on compliance for the year ended June 30, 2017, as finding 2017-04.

Agency Response: Concur

Agency: University of Arizona
Name of contact person and title: Lanita Collete, Chief Information Officer
Anticipated completion date: May 2018

The University acknowledges the need to improve our information security practices. The University currently plans to hire additional personnel to appropriately staff the Information Security Office. Once hiring and training is complete, we will have improved ability to handle monitoring, detection, response, contingency-planning, and recovery/lessons learned.

2017-21
The University of Arizona should improve its contingency planning procedures for its information technology resources

Criteria—It is critical that the University of Arizona (University) 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 enterprise 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 system and data backup policies and procedures.

Condition and context—Although the University was performing system and data backups, it did not have documented policies and procedures for testing them to ensure they were operational and could be used to restore its IT resources.

Effect—The University 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 University's contingency planning policies and procedures need further development to ensure its disaster recovery efforts can be relied on in the event they are needed.

Recommendations—To help ensure university operations continue in the event of a disaster, system or equipment failure, or other interruption, the University should establish and document policies and procedures for testing IT system software and data backups to help ensure they could be recovered if needed. The University should review its contingency-planning procedures against current IT standards and best practices and implement them university-wide, as appropriate. Further, the University should train staff on the policies and procedures.

The University of Arizona's responsible officials' views and planned corrective action are in its corrective action plan included in the Universities Responses section at the end of this report. This finding was also reported in the University of Arizona's separately issued report on internal control and on compliance for the year ended June 30, 2017, as finding 2017-05.

Agency Response: Concur

Agency: University of Arizona
Name of contact person and title: Lanita Collete, Chief Information Officer
Anticipated completion date: May 2018

We acknowledge that a backup testing plan is necessary as part of the contingency planning and will develop appropriate policies and procedures for testing to ensure successful recovery from backups.

2017-22
Significant audit adjustment

Criteria—Internal controls should be in place to provide reasonable assurance that expenses and revenues are recorded in the proper period in accordance with U.S. GAAP.

Condition and context—During the course of our audit, we proposed and the Department subsequently recorded a significant adjustment to correct accounts receivable/revenue and accounts payable/expenses. As a result of audit procedures, we noted that 4 transactions were not recorded in the proper period. We proposed and the Department subsequently recorded an adjustment to accrue right-of-way condemnation judgments, which resulted in adjustments to accounts payable and related expenses as well as federal reimbursement receivables and related revenues as a recognizable subsequent event.

Effect—The lack of controls in place over the review of contingent liabilities and subsequent disbursements increases the risk of misstatements or errors occurring and not being detected and corrected.

Cause—The Department has not adopted a policy to review right-of-way transactions for contingent liabilities. As such the Department did not properly accrue right-of-way condemnation judgments. Management is in the process of implementing controls and procedures.

Recommendations—We recommend that the Department implement policies and proper internal control procedures to ensure that expenditures are recorded in the proper period.

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

Agency Response: Concur

Agency: Department of Transportation
Name of contact person and title: Tim Newton, Controller
Anticipated completion date: Unknown

The Arizona Department of Transportation (ADOT) concurs with the finding and will address concerns by September 30, 2018 by developing policies and procedures that will provide reasonable, but not absolute, assurance that material unrecorded receivables, liabilities, and related revenues and expenditures are accrued in the proper accounting period, subject to the State's 60 day availability criteria for reporting liabilities in the governmental fund financial statements. These policies and procedures will also include detailed procedures to ensure proper accrual of material unrecorded receivables, liabilities, and related revenues and expenditures on the full-accrual basis of accounting.