Financial Statement Findings and State Responses
(Reformatted from the FY 2019 Report on Internal Control and Compliance)

2019-01
Managing risk

Condition and context— We reviewed the risk-assessment process at 4 State agencies including the Departments of Administration (ADOA), Economic Security (DES), Child Safety (DCS), and Revenue (DOR) and found that the agencies' processes for managing and documenting their risks did not include an overall risk-assessment process that included identifying, analyzing, and responding to the agency-wide information technology (IT) risks, such as potential harm from unauthorized access, use, disclosure, disruption, modification, or destruction of IT data and systems. Also, the agencies' processes did not include identifying, classifying, and inventorying sensitive information that might need stronger access and security controls and evaluating and determining the business functions and IT systems that would need to be restored quickly if the agencies were impacted by disasters or other system interruptions.

Criteria— Effectively managing risk at State agencies includes each agency establishing an entity-wide risk-assessment process that involves members of its administration and IT management to determine the risks the agency faces as it seeks to achieve its objectives to not only report accurate financial information and protect its IT systems and data but to also carry out its overall mission and service objectives. The process should provide the basis for developing appropriate responses based on identified risk tolerances and specific potential risks to which the agency might be subjected. To help ensure the agency's objectives can be met, an annual risk assessment should consider IT risks. For each identified risk, the agency should analyze the identified risk and develop a plan to respond within the context of the agency's defined objectives and risk tolerances. The process of managing risks should also address the risk of unauthorized access and use, modification, or loss of sensitive information and the risk of losing the continuity of business operations in the event of a disaster or system interruption.

Effect— Without correcting these deficiencies, the State agencies' administration and IT management may put the agencies' operations and IT systems and data at unintended and unnecessary risk.

Cause— Because the State's risk-assessment process is decentralized and managed at each agency, the agencies are in various stages of developing or implementing policies and procedures for assessing and managing risk and have not fully implemented agency-wide risk-assessment processes that address IT security. Additionally, DCS fully relies on the DES to perform the risk assessment over its IT system and network, and DCS does not coordinate efforts to ensure its system is properly evaluated.

Recommendations— State agencies should identify, analyze, and reduce risks to help prevent undesirable incidents and outcomes that could impact business functions and IT systems and data. They should also plan for where to allocate resources and where to implement critical controls. To help ensure they have effective agency-wide policies and procedures to achieve these objectives, the State agencies should follow guidance the Arizona Strategic Enterprise Technology Office established, which is based on the IT security framework of the National Institute of Standards and Technology. Responsible administrative officials and management over finance, IT, and other agency functions should be asked for input in the agencies' process for managing risk. State agencies should conduct the following as part of their process for managing risk:

- Perform an annual agency-wide IT risk-assessment process that includes evaluating and documenting risks and safeguards. Such risks may include inappropriate access that would affect financial data, system changes that could adversely impact or disrupt system operations, and inadequate or outdated system security. (DES, DCS, DOR)
- Evaluate and manage the risks of holding sensitive information by identifying, classifying, and inventorying the information the agency holds to assess where stronger access and security controls may be needed to protect data in accordance with State statutes and federal regulations. (ADOA, DES, DCS)
- Evaluate and determine the critical organization functions and IT systems that would need to be restored quickly given the potential impact disasters or other IT system interruptions could have on the organization's operations, such as public assistance and safety, payroll, and accounting, and determine how to prioritize and plan for recovery. (ADOA, 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 2018-01.

Agency Response: Concur

Agency: Department of Administration
Name of contact person and title: Ray Di Ciccio, Interim Comptroller
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. The State has developed policies and procedures and will be documenting additional processes. Each agency has developed a detailed corrective action plan to address this finding.

2019-02
Information technology (IT) controls—access, configuration management, security, and contingency planning

Condition and context— We reviewed the access, configuration management, information technology security, and contingency-planning controls at 4 State agencies including the Departments of Administration (ADOA), Economic Security (DES), Child Safety (DCS), and Revenue (DOR) and found that 3 of the 4 agencies' control procedures were not sufficiently designed, documented, and implemented to respond to risks associated with their IT systems and data. DCS relies on DES for access, configuration management, and security and relies wholly on DES for contingency planning because its systems and data are housed on DES' network. The agencies lacked adequate procedures over the following:

- **Restricting access to their IT systems and data**—Procedures did not consistently help prevent or detect unauthorized or inappropriate access. (ADOA, DES, DOR)
- **Configuring systems securely and managing system changes**—Procedures did not ensure all IT system changes were adequately managed and configuration settings maintained. (DES)
- **Securing systems and data**—IT security policies and procedures lacked controls to prevent unauthorized or inappropriate access or use, manipulation, damage, or loss.. (ADOA, DES, DOR)
- **Developing and documenting, testing, and updating a contingency plan**—Plans lacked key elements related to restoring operations in the event of a disaster or other system interruption, did not require the contingency plan to be tested, and were not updated, as necessary. (ADOA, DES, DOR)

Criteria—State agencies should have effective internal controls to protect their IT systems and help ensure the integrity and accuracy of the data they maintain.

- **Logical and physical access controls**— Help to ensure systems and data are accessed by users who have a need, systems and data access granted is appropriate, key systems and data access is monitored and reviewed, and physical access to its system infrastructure is protected. (ADOA, DES, DOR)
- **Well-defined, documented configuration management process**—Ensures the IT system configurations are documented and that changes to the systems are identified, documented, evaluated for security implications, tested, and approved prior to implementation. This helps limit the possibility of an adverse impact on the system's security or operation. Separating responsibilities is an important control for system changes; the same person who has authority to make system changes should not put the change into production. If those responsibilities cannot be separated, a post-implementation review should be performed to ensure the change was implemented as designed and approved. (DES)
- **IT security internal control policies and procedures**—Help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to IT systems and data. (ADOA, DES, DOR)
- **Comprehensive, documented, and tested contingency plan**—Provides the preparation necessary to place the plan in operation and helps to ensure business operations continue and systems and data can be recovered in the event of a disaster, system or equipment failure, or other interruption. (ADOA, DES, DOR)

Effect— There is an increased risk that the State agencies may not adequately protect their IT systems and data, which could result in unauthorized or inappropriate access and/or the loss of confidentiality or integrity of systems and data. It also increases the agencies' risk of not being able to effectively continue daily operations and completely and accurately recover vital IT systems and data in the event of a disaster or system interruption.

Cause— Because the State is decentralized and IT systems and data are managed at each agency, the State agencies are in various stages of developing and implementing policies and procedures for access, configuration management, security, and contingency planning and, because of a lack of resources, have not fully implemented them.

Recommendations— To help ensure the State agencies have effective policies and procedures over their IT systems and data, agencies should follow guidance the Arizona Strategic Enterprise Technology Office established, which is based on the IT security framework of the National Institute of Standards and Technology. To help achieve these control objectives, the agencies should develop, document, and implement control procedures as applicable in each IT control area described below:

Access

- Assign and periodically review employee user access ensuring appropriateness and compatibility with job responsibilities. (ADOA, DES, DOR)
- Remove terminated employees' access to IT systems and data. (ADOA, DES, DOR)
- Review all other account access to ensure it remains appropriate and necessary. (ADOA, DES, DOR)
- Evaluate the use and appropriateness of accounts shared by 2 or more users and manage the credentials for such accounts. (DES, DOR)
- Enhance authentication requirements for IT systems. (DES, DOR)
- Review data center physical access periodically to determine appropriateness. (ADOA)

Configuration and change management

- Maintain configurations for all system services, assets, and infrastructure; manage configuration changes; and monitor the system for unauthorized or unintended configuration changes. (DES)

Security

- Perform proactive key user and system activity logging and log monitoring, particularly for users with administrative access privileges. (ADOA, DOR)
- Prepare and implement a security incident response plan clearly stating how to report and handle such incidents. (DES)
- Develop, document, and follow a process for awarding and subsequent monitoring of IT vendor contracts. (ADOA, DES)

Contingency planning

- Update the contingency plan and ensure it includes all critical elements to restore critical operations, including being prepared to move critical operations to a separate alternative site if necessary. (ADOA)
- Develop and implement a contingency plan and ensure it includes all required elements to restore critical operations, including being prepared to move critical operations to a separate alternative site if necessary. (DOR)
- Test the contingency plan. (DES, DOR)
- Train staff responsible for implementing the contingency plan. (ADOA, 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 findings 2018-02 and 2018-03.

Agency Response: Concur

Agency: Department of Administration
Name of contact person and title: Ray Di Ciccio, Interim 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. Policies and procedures have been implemented or are being developed to address any gaps. Each agency has developed a detailed corrective action plan to address this finding.

2019-03
The State's process for reporting cash and investments was not adequate to prevent misstatements in the State's financial statements, which increases the risk that those relying on the reported financial information could be misled

Condition and context— The State Treasurer's Office (STO) and Arizona Department of Administration's (ADOA) process to reconcile cash and investments between the STO's investment management system and the State's accounting system did not always accurately identify differences between the systems. Therefore, their process did not ensure appropriate adjusting journal entries were made in the State's financial system to correct any imbalances so that all cash and investments activity was properly reflected in the State's financial statements.

Criteria— ADOA is required to maintain complete, accurate, and current financial records of the State's cash and investments in order to prepare the State's financial statements in accordance with generally accepted accounting principles. (Arizona Revised Statutes §35-131(B)) To help ensure ADOA's records of cash and investments are accurate, the STO and ADOA should reconcile their systems and investigate and resolve any imbalances and errors in a timely manner.

Effect— Those relying on financial information in the State's financial statements may have been misled because the State misstated the Land Endowment Fund's earnings on investments and ending investment balance in its final 2018 and draft 2019 financial statements. These amounts were understated by $85 million in the State's 2018 financial statements and overstated by $45 million in the State's 2019 draft financial statements. The State adjusted its 2019 financial statements for these material misstatements.

Cause— The STO did not have proper controls to ensure adjusting journal entries that it recommended to ADOA for compilation of the State's financial statements were appropriate, correct, and reviewed for propriety. In addition, there was a lack of communication between the STO and ADOA during the reconciliation process.

Recommendations— To ensure that the State's cash and investments recorded on the STO's investment management system and the State's accounting system are fully reconciled and the State's financial statements are accurately presented, the STO and ADOA must work together to improve their process and develop written procedures that ensure:

- A joint reconciliation is performed on a regular basis with both the STO and ADOA and differences noted during the reconciliation process are investigated and resolved in a timely manner.
- Someone at STO with knowledge of both systems and who is independent of the journal entries preparation performs a detailed review of the monthly and year-end journal entries for propriety.
- Year-end journal entries the STO recommends for fair presentation of the State's financial statements are reviewed and approved by ADOA to verify their accuracy.

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 Administration and State Treasurer's Office
Name of contact persons and title: Ray Di Ciccio, Interim Comptroller
Jackie Harding, Deputy Treasurer of Operations
Anticipated completion date: Unknown

The State Treasurer's Office (STO) and Arizona Department of Administration (ADOA) are meeting monthly to discuss and implement improvements to this process including knowledge transfer, training and more frequent reconciliation. Additionally, STO is currently updating their internal documentation and general ledger system. Further, we note STO received a clean audit on its financial statements, and this finding has to do with reconciling the STO general ledger with the ADOA accounting system.

2019-04
The Department of Revenue did not ensure it collected all income taxes that are due to the State

Condition and context— The Department of Revenue (DOR) failed to reconcile State income taxes to ensure all amounts due from taxpayers were collected and accurately reported in the State's financial statements. This finding has been reported since fiscal year 2006.

Criteria— DOR is the State agency that has the sole responsibility for collecting and reporting all the State's income taxes and should have adequate procedures and systems in place to do so.

Effect— There is an increased risk that the State may not collect all income taxes that are due. Also, the State risks reporting inaccurate income tax revenue in its financial statements.

Cause— DOR's tax administration system lacked the functionality to perform automatic system checks and reconciliations, and DOR did not have the resources to perform manual compensating review procedures.

Recommendations— To help ensure DOR collects all State income taxes that are due from taxpayers and accurately reports this revenue in the State's financial statements, it should either fix its system's limitations so that the system automatically checks and reconciles income taxes or immediately implement other processes to reconcile income taxes.

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 2018-05.

Agency Response: Concur

Agency: Department of Revenue
Name of contact person and title: Mike Devine, ADOR Chief Internal Auditor
Anticipated completion date: June 2020

For the 2019 tax year, the Department is piloting a project to compare W-2 withholding data from employers to the amount of withholding reported by taxpayers. When discrepancies are identified, the Department is sending letters to the taxpayers requesting that they review their return information. The Department is also working on a project to develop methods to collect and capture W-2 and Form 1099 data and develop a tool to perform a reconciliation process for withholding and individual income taxes. The Department plans to complete this project by the end of fiscal year 2020.

2019-05
The Department of Revenue has not published $17 million of unclaimed individual income tax overpayments, dating back as far as 2007, as abandoned property on its website for taxpayers to search and claim

Condition and context— The Department of Revenue (DOR) did not include $17 million of individual income tax overpayments in its unclaimed property system that is used to publish abandoned property on its website for taxpayers to search and claim. These overpayments, from 46,265 taxpayer accounts, ranged from $50 to $269,917 and date back as far as fiscal year 2007. Taxpayers have approximately 35 years to file a claim for abandoned property. (A.R.S. §44-317(E)) The State included these abandoned overpayments as a liability in its financial statements.

Criteria— DOR must publish information about all abandoned property of at least $50 on its website, including information about unclaimed individual income tax overpayments. (A.R.S. §44-309)

Effect— Abandoned individual income tax overpayments may not be readily available for individual taxpayers to search and claim.

Cause— DOR's tax administration system lacked the functionality to automatically transfer individual income tax overpayments from that system to its unclaimed property system and DOR did not have sufficient resources to do so manually.

Recommendation— To ensure taxpayers can search and claim individual income tax overpayments, DOR should develop and implement a process to publish abandoned overpayments of at least $50 on its website. The process should include policies and procedures to ensure the overpayments are properly accounted for in the unclaimed property system and tax administration system.

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: Mike Devine, ADOR Chief Internal Auditor
Anticipated completion date: Unknown

As noted in the finding, issues with ADOR's tax administration system currently prevent the Department from transferring overpayments to the unclaimed property system. However, information regarding these overpayments is still accessible by taxpayers that call in to the Department. In February 2020, the Department contracted for a feasibility study for replacing the tax administration system. This study will assess the Department's current tax system, develop the scope of work necessary for procuring a new tax system, and identify funding options for the new tax system. The Department will use this study to develop a budget request for a new tax system. The study should be completed by the end of June 2020. As a part of the initiative to replace the existing system, the Department is currently engaged in a data cleanup project that includes addressing abandoned overpayments.

2019-06

The Arizona Department of Administration and PSPRS did not adequately communicate and work together to ensure the accuracy of CORP's ADC employee data provided to actuaries, which increases the risk that those relying on the pension liability reported in the State's financial statements could be misled and future employer contributions will be inadequate to cover future benefit payments

Condition and context— The Arizona Department of Administration (ADOA) and the Public Safety Personnel Retirement System (PSPRS) did not adequately communicate and work together to ensure the accuracy of employee personnel data maintained by PSPRS for its members in the Corrections Officer Retirement Plan (CORP) for the Arizona Department of Corrections (ADC), resulting in inaccuracies of data maintained by PSPRS and provided to its actuaries. Inaccuracies of employee personnel data, such as salary, hire date, birthdate, and years of credited service, used by the actuaries increases the risk that they could incorrectly estimate the pension liability and the employer required contribution rate needed to cover CORP's ADC members' future benefit payments.

Criteria— PSPRS administers the CORP for ADC members and uses its records of CORP's ADC active employee personnel data to provide to its actuaries so they can calculate the estimated total pension liability and other pension amounts reported in the State's financial statements and to determine employer contribution rates. The State's payroll system includes the records of this personnel data for CORP members who are actively employed with ADC. Therefore, it is critical that ADOA and PSPRS communicate and work together to ensure the employee personnel data the actuaries are given is accurate.

Effect— There is an elevated risk that the estimated pension liability reported in the State's financial statements could be significantly misstated and mislead those relying on the information. There is also an increased risk that CORP's employer contribution rates could be inadequate to cover future benefit payments. Although for the most recent 2018 actuarial report, PSPRS provided inaccurate data for some of CORP's ADC active members, the discrepancies were not enough to cause any significant errors in the actuaries' calculations.

Cause— ADOA and PSPRS did not have policies and procedures in place to reconcile CORP's active employee personnel data for ADC between its payroll system and PSPRS' records.

Recommendations— To help ensure that the State's pension amounts presented in its financial statements are accurate and do not mislead those relying on the information and CORP's ADC employer contributions are adequate to cover future benefit payments, ADOA and PSPRS should:

- Annually reconcile CORP's ADC active employee personnel data between the State's payroll records and PSPRS' records and investigate and resolve any errors prior to PSPRS providing the information to its actuaries.
- Determine the most appropriate time to perform this reconciliation in order for PSPRS to ensure it provides accurate information to its actuaries.
- Retain a copy of the reconciliation.

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

Agency's response: Concur

Agency: Department of Administration and Public Safety Personnel Retirement System
Name of contact persons and titles: Ray Di Ciccio, Interim Comptroller
Mike Townsend, Administrator and Michael Smarik, Deputy Administrator

Anticipated completion date: September 2020

The Department of Administration and the Public Safety Personnel Retirement System will collaborate on establishing procedures to ensure the accuracy of employee data reported to actuaries.

2019-07
University of Arizona—Managing risk

Condition and context— The University of Arizona's (UA) process for managing and documenting its risks did not include an overall risk assessment process that included identifying, analyzing, and responding to the university-wide information technology (IT) risks, such as potential harm from unauthorized access, use, disclosure, disruption, modification, or destruction of IT data and systems. Also, it did not include identifying, classifying, and inventorying sensitive information that might need stronger access and security controls.

Criteria— Effectively managing risk at the UA includes an entity-wide risk assessment process that involves members of the UA's administration and IT management to determine the risks the UA faces as it seeks to achieve its objectives to not only report accurate financial information and protect its IT systems and data but to also carry out its overall mission and service objectives. The process should provide the basis for developing appropriate responses based on identified risk tolerances and specific potential risks to which the UA might be subjected. To help ensure the UA's objectives can be met, an annual risk assessment should consider IT risks. For each identified risk, the UA should analyze the identified risk and develop a plan to respond within the context of the UA's defined objectives and risk tolerances. The process of managing risks should also address the risk of unauthorized access and use, modification, or loss of sensitive information.

Effect— Without correcting these deficiencies, the UA's administration and IT management may put the UA operations and IT systems and data at unintended and unnecessary risk.

Cause— The UA has started to conduct a risk assessment process on its significant enterprise systems that includes implementation of its existing data-classification policy. However, time and resource limitations have not allowed the UA to fully implement prior-year recommendations to effectively manage IT risk.

Recommendations— The UA should identify, analyze, and reduce risks to help prevent undesirable incidents and outcomes that could impact IT systems and data. It also should plan for where to allocate resources and where to implement critical controls. To help ensure it has effective entity-wide policies and procedures to achieve these objectives, the UA should follow guidance from a credible industry source, such as the National Institute of Standards and Technology. Responsible administrative officials and management over finance, IT, and other entity functions should be asked for input in the UA's process for managing risk. The UA should conduct the following as part of its process for managing risk:

- Perform an annual entity-wide IT risk-assessment process that includes evaluating and documenting risks and safeguards. Such risks may include inappropriate access that would affect financial data, system changes that could adversely impact or disrupt system operations, and inadequate or outdated system security.
- Evaluate and manage the risks of holding sensitive information by identifying, classifying, and inventorying the information the UA holds to assess where stronger access and security controls may be needed to protect data in accordance with State statutes and federal regulations.

The UA'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 UA's separately issued report on internal control and on compliance for the year ended June 30, 2019, as finding 2019-01.

This finding is similar to prior-year finding 2018-09.

Agency Response: Concur

Agency: University of Arizona
Contact Person: Lanita Collette, Chief Information Security Officer
Anticipated completion date: June 30, 2020

The university will complete risk assessment processes for all enterprise applications by June 30, 2020 including the identification, inventory and classification of data.

The policy and process designate responsibility for executing the process to Information Owners and Information System Owners and makes the Information Security Office accountable for developing, testing, reviewing, and maintaining a university-wide Information Security Plan that incorporates elements of the security plans created and approved by Information Owners and Information System Owners.

This new process allows for the effective management of information security risk through steps for:

- Data collection, including inventory and classification (by criticality and sensitivity) of information resources, identification of stakeholders (from both business and technical positions in the university) and designation of accountability, and analysis of business impacts.
- Risk assessment, with assessment questions based upon the NIST CSF, incorporating elements of confidentiality, integrity, and availability, and tailored to be more meaningful in the environment of higher education.
- Risk analysis that incorporates insights into business impacts, the threat landscape, and an understanding of the traceability between vulnerabilities and threats, to ensure meaningful and consistent risk ranking.
- Security planning that clarifies and documents explicit decisions (within a risk register), based upon risk tolerances of Information Owners and Information System Owners, related to risk handling including choices to accept, transfer, avoid, or mitigate.

The process has been defined as an ongoing activity, for units, with re-assessment and security plan revision occurring at least annually. Production of the University Security Plan will be an annual occurrence, aligned with the fiscal year.

2019-08
University of Arizona's Information technology (IT) controls—security and contingency planning

Condition and context— The University of Arizona's (UA) control procedures were not sufficiently designed, documented, and implemented to respond to risks associated with its IT systems and data. The UA lacked adequate procedures over the following:

- **Securing systems and data**—Policies and procedures did not require the logging and monitoring of elevated user activities within the UA's enterprise systems.
- **Developing and documenting a comprehensive contingency plan**—Plan lacked restoration processes for 2 of the 4 significant enterprise systems, and a copy of the plan was not readily available outside the IT systems.

Criteria— The UA should have effective internal controls to protect its IT systems and help ensure the integrity and accuracy of the data it maintains.

- **IT security internal control policies and procedures**—Help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT systems and data.
- **Comprehensive, documented, and tested contingency plan**—Provides the preparation necessary to place the plan in operation and helps to ensure business operations continue and systems and data can be recovered in the event of a disaster, system or equipment failure, or other interruption.

Effect— Without correcting these deficiencies, there is an increased risk that the UA may not adequately protect its IT systems and data, which could result in unauthorized or inappropriate access and/or the loss of confidentiality or integrity of systems and data. It also increases the UA's risk of not being able to effectively continue daily operations and completely and accurately recover vital IT systems and data in the event of a disaster or system interruption.

Cause— The UA created work group has not completed its development of logging and monitoring policies and procedures. Further, due to time and resource constraints, the UA completed disaster recovery plans for only 2 of its 4 significant enterprise systems.

Recommendations— To help ensure the UA has effective policies and procedures over its IT systems and data, the UA should follow guidance from a credible industry source such as the National Institute of Standards and Technology. To help achieve these control objectives, the UA should develop, document, and implement control procedures in each IT control area described below

Security

- Perform proactive key user and system activity logging and log monitoring, particularly for users with administrative access privileges.

Contingency planning

- Develop and implement a contingency plan for the remaining 2 significant UA enterprise systems.
- Test the contingency plan.
- Train staff responsible for implementing the contingency plan.
- Maintain a readily accessible copy of the plan.

The UA'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 UA's separately issued report on internal control and on compliance for the year ended June 30, 2019, as finding 2019-02.

This finding is similar to prior-year findings 2018-10.

Agency Response: Concur

Agency: University of Arizona
Contact Person: Lanita Collette, Chief Information Security Officer

Anticipated completion date: Logging and Monitoring is an on-going activity. Contingency planning for the remaining two applications will be completed by June 30, 2020, as well as system activity logging and log monitoring, particularly for users with administrative access privileges.

On August 23, 2019, the Audit, Accountability, and Activity Review Standard took effect. This standard supports the corresponding policy and establishes requirements for:

- Responsibility for ensuring log events are captured and monitored;
- The definition of log collection and aggregation systems;
- The collection and retention of logs; and
- Reporting of logging and monitoring related data to the Information Security Office.

Additionally, Information Security Policy Training is under development and is designed to help stakeholders understand their responsibilities for protecting university data; including their responsibility to support log collection and aggregation and to perform review of reports derived from these logs.

By June 30, 2020, the university will ensure stronger access and security controls are in place to protect data in accordance with State statutes and federal regulations, with essence on individuals with elevated privileges. An annual review will be put in place to ensure access and security controls are in place to protect data.

By June 30, 2020, the university will have developed and documented contingency plans for the remaining two significant university enterprise systems. The university testing of its backup procedures aligns with the movement of enterprise web applications to cloud services. The university will move forward to address the business impacts within the two applications, which were not covered in fiscal year 2019, identifying critical IT systems that will need to be restored quickly in the event of disruption. Documented procedures will be created, staff will be trained, and the university will maintain a readily accessible copy of the plans for all enterprise applications. In addition, our cloud service provider has failover and recovery capabilities in the event of a disaster, system or equipment failure, or other interruption. We do use multi-availability zones for our enterprise systems. As part of the cloud services functionality, snapshots are taken from production and they are staged in a different environment, validating their viability. Our provider has redundancy and failover built into their network and infrastructure, plus the university has the ability to build the environment from scratch if needed with these snapshots.

2019-09
PSPRS' inadequate controls over the financial statement compilation process

The other auditors who audited the Public Safety Personnel Retirement System (PSPRS) reported the following internal control deficiency over PSPRS' financial statement compilation process for activity that is reported within the Pension and Other Employee Benefit Trust Funds in the State's financial statements. PSPRS' and the State's 2019 financial statements were adjusted for all material misstatements noted.

Condition and context— Management did not have adequate internal control procedures in place over the financial statement reporting process using the basis of accounting required by generally accepted accounting principles (GAAP). A number of month-end and year-end close-out items were identified during the audit of the financial statements. While management and staff have an understanding of general ledger controls and plan compliance requirements, sufficient internal controls were not designed and operating to properly prevent misstatements in the financial statements.

During our review of the PSPRS financial statements, we noted the following:

- PSPRS's financial reporting database does not have a consolidated general ledger module.
- PSPRS's financial reporting database does not allow for accounting periods to be closed and locked from transactions and journal entries.
- PSPRS's financial reporting database does not allow for bank reconciliations to be accurately completed and reviewed in a timely, efficient manner.
- Cash and short-term investments totaling approximately $1,180,984 were reported as other receivables in the financial statements.
- Several asset and liability balances were not reviewed at year-end to ensure that the proper balance or accrual reflected current fiscal year activity; assets totaled approximately $5,250,907 and liabilities totaled approximately $1,310,654.
- Employer contributions were overstated, and employee contributions were understated by approximately $3,925,791 for contribution made by the employer on the employee's behalf.
- Net appreciation in fair value and investment expenses were overstated by approximately $3,125,553.

Criteria— Management is responsible for designing, implementing, and maintaining internal controls that include controls over the general ledger and complete and accurate financial statements.

Effect— PSPRS's internal controls over financial reporting at the financial statement level were not designed and operating to ensure that a misstatement would be prevented or detected and corrected in a timely manner.

Cause— PSPRS experienced significant turnover in key positions, changed financial-reporting databases in the prior year, and lacked documented policies and procedures for month-end and year-end closing.

Recommendations— PSPRS should design and implement effective internal control procedures to ensure the financial statements are free from misstatements and consistent with accounting policies. Additionally, PSPRS should allocate the necessary staffing and information technology resources to implement and maintain controls and procedures for month-end and year-end closing.

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

Agency's Response: Concur

Agency: Public Safety Personnel Retirement System
Name of contact persons and titles: Mike Townsend, Administrator
Mike Smarik, Deputy Administrator
Anticipated completion date: September 2020

Public Safety Personnel Retirement System (PSPRS) will review its internal controls and make necessary improvements. An Audit Committee was established in October 2019, which will oversee the implementation of internal control enhancements. Additionally, PSPRS will implement a new General Ledger system that will help to ensure effective internal controls are in place and allow for month and year-end closing.

2019-10
Internal Controls for Revenue and Fuel Tax Administration Department

The other auditors who audited the Arizona Department of Transportation (ADOT) reported the following internal control deficiency over cash receipting and reconciliation for the Revenue and Fuel Tax Administration Department that processes highway user revenue monies and fuel taxes that are reported within the Other Governmental Funds in the State's financial statements.

Condition and context— Each employee within the Revenue and Fuel Tax Administration Department (RFTA) has access to cash/checks prior to deposit and has the ability to add/edit bank statement information within the MAX system. The MAX system is used to reconcile bank data to the receipts data.

Criteria— Internal controls should be in place to provide reasonable assurance that the duties of cash receipting are segregated from the reconciliation process.

Effect— The lack of controls in place over the cash receipting and reconciliation process increases the risk of the misappropriation of cash occurring and not being prevented or detected.

Cause— RFTA has not properly implemented procedures within RFTA to ensure the proper segregation of duties. Management is in the process of implementing controls and procedures.

Recommendations— We recommend that RFTA implement policies and proper internal control procedures to ensure that the duties of cash receipting are segregated from the reconciliation process.

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, Deputy CFO
Anticipated completion date: January 31st, 2020

Response: The Arizona Department of Transportation (ADOT) concurs with the finding and is in the process of transitioning the cash handling function from RFTA to MVD. It is anticipated this transition will be complete by 1/31/2020. Upon completion the cash handling duties for all of the business units located at 1801 W. Jefferson will be transitioned to an MVD unit who does not have any reconciliation or transactional ability. Business units at 1801 will bring any cash and check deposits to the MVD unit. They will receipt for the deposits to the business unit, compile all cash deposits, and coordinate the Loomis pickup. Any checks received by 1801 business units will be sent to receipts accounting unit for scanning and depositing with BOA.

Both MVD and FMS will do a weekly reconciliation between the cash receipts and Loomis pickup log. Standard work will be developed with MVD before transition of cash handling is completed.