Financial Statement Findings and State Responses
(Reformatted from the FY 2018 Report on Internal Control and Compliance)

2018-01
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' risk-management processes did not include an overall risk-assessment process that included identifying, analyzing, and responding to 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 agency-wide risk-assessment process involving 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 include considering 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 risk-management process should also address the risk of unauthorized access, 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— 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 relies partly on DES for assessing and managing risk over its systems and data because they are housed on DES' network.

Recommendations— State agencies should identify, analyze, and reduce risks to help prevent undesirable incidents and outcomes that could impact business functions, IT systems, and data. They also should plan for where resources should be allocated and where critical controls should be implemented. To help ensure they have effective agency-wide policies and procedures to achieve these objectives, State agencies should follow guidance established by the Arizona Strategic Enterprise Technology Office, 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 risk-management process. State agencies should conduct the following as part of their risk-management process:

- Perform an annual agency-wide IT risk-assessment process that includes evaluating risks, such as risks of inappropriate access that would affect financial data, system changes that could adversely impact or disrupt system operations, and inadequate or outdated system security. (ADOA, 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, DOR)
- Evaluate and determine the business functions and IT systems that would need to be restored quickly given the potential impact disasters or other IT system interruptions could have on critical organizational functions, such as public assistance and safety, operations, and payroll and accounting, and determine how to prioritize and plan for recovery. (ADOA, 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 2017-01.

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. 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.

2018-02
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 the agencies' control procedures were not sufficiently designed, documented, and implemented to respond to risks associated with their IT systems and data. The agencies lacked adequate procedures over the following:

- Restricting access to IT systems and data—Procedures did not consistently help prevent or detect unauthorized or inappropriate access. (ADOA, DES, DCS, DOR)
- Configuring systems securely and managing system changes—Procedures did not ensure IT systems were securely configured and all changes were adequately managed. (ADOA, DES, DOR)
- 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 or updating a contingency plan—Plan either was not in place for restoring operations in the event of a disaster or other system interruption or it lacked key elements necessary to succeed in restoring operations. (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 system infrastructure is protected. (ADOA, DES, DCS, DOR)
- Well-defined documented configuration management process—Ensures IT systems are configured securely 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 security or operations. Separation of 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. (ADOA, DES, DOR)
- 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 State agencies may not adequately protect their IT systems and data, which could result in unauthorized or inappropriate access and the loss of confidentiality and 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. Additionally, DCS relies partly 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.

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

Access

- Assign and periodically review employee user access ensuring appropriateness and compatibility with job responsibilities. (ADOA, DES, DCS, DOR)
- Remove terminated employees' access to IT systems and data. (ADOA, DCS, DOR)
- Review all other account access to ensure it remains appropriate and necessary. (ADOA, DES, DCS, DOR)
- Evaluate the use and appropriateness of accounts shared by 2 or more users and manage the credentials for such accounts. (ADOA, DES, DOR)
- Enhance authentication requirements for IT systems. (ADOA)
- Manage employee-owned and entity-owned electronic devices connecting to the agency's systems and data (DOR))
- Manage remote access to the agency's systems and data. (ADOA, DCS, DOR)
- Utilize data-sharing agreements when sharing the agency's data, limit the access as appropriate, and enforce data-sharing security restrictions. (DOR)
- Review data center physical access periodically to determine whether individuals still need it. (ADOA, DOR)

Configuration and change management

- Establish and follow a documented change management process. (DOR)
- Review proposed changes for appropriateness, justification, and security impact. (DOR)
- Document changes, testing procedures and results, change approvals, and post-change review. (DOR)
- Develop and document a plan to roll back changes in the event of a negative impact to IT systems. (DOR)
- Test changes prior to implementation. (DOR)
- Separate responsibilities for the change management process or, if impractical, perform a post-implementation review to ensure the change was implemented as approved. (DOR)
- Configure IT resources appropriately and securely and maintain configuration settings. (ADOA, DES, DOR)
- Manage software installed on employee computer workstations. (DES, DOR)

Security

- Perform proactive key user and system activity logging and log monitoring, particularly for users with administrative access privileges. (ADOA, DES, DOR)
- Prepare and implement a security-incident-response plan clearly stating how to report and handle incidents. (DES, DOR)
- Provide all employees ongoing training on IT security risks and their responsibilities to ensure systems and data are protected. (DOR)
- Perform IT vulnerability scans and remediate vulnerabilities in accordance with a remediation plan. (ADOA, DES, DOR)
- Identify, evaluate, and apply patches in a timely manner. (ADOA, DES, DOR))

Contingency planning

- Develop and implement a contingency plan or update the contingency plan if a plan is in place, and ensure it includes all required elements to restore critical operations, including being prepared to enable moving critical operations to a separate alternative site if necessary. (ADOA, DES, DOR)
- Test the contingency plan. (ADOA, DES, DOR)
- Test the contingency plan. (ADOA, DES, DOR)
- Train staff responsible for implementing the contingency plan. (ADOA, DES, DOR)
- Back up and securely maintain backups of systems and data. (ADOA, 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 findings 2017-02 (access), 2017-03 (configuration and change management), 2017-04 (IT security), and 2017-05 (contingency planning).

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.

2018-03
The Department of Administration's Data Center contracts with State agencies are missing key elements

Condition and context— The Department of Administration's Data Center's IT service contracts with State agencies did not adequately specify the extent of backup and recovery services that would be provided in the event of a disaster or other system interruptions. Also, the contracts lacked responsibilities and priorities for restoring operations, including what systems and data, if any, an agency would need to provide to the Data Center to successfully restore its operations.

Criteria— IT service contracts between the Data Center and other State agencies should be complete and up to date and include the agencies' responsibilities and priorities for recovery efforts to help ensure that Arizona Auditor General State of Arizona—Schedule of Findings and Questioned Costs | Year Ended June 30, 2018 PAGE 13 expectations on the extent of services provided are clear and operations can be fully restored in the event of a disaster, system or equipment failure, or other interruption.

Effect— There is an increased risk that agencies may not understand the extent of backup and recovery services the Data Center will provide, and the Data Center may not be able to fully restore agencies' systems and data in the event of a disaster, system or equipment failure, or other interruption.

Cause— The Data Center did not have sufficient policies and procedures in place to help ensure that IT service contracts with State agencies sufficiently addressed the extent of services and the agencies' responsibilities and priorities for recovery efforts and that the contracts were updated as needed.

Recommendations—To help ensure its IT service contracts with other State agencies are effective in restoring agencies' operations in the event of a disaster, system or equipment failure, or other interruption, the Data Center should:

- Improve its policies and procedures for contracting IT services with other State agencies to ensure that the contracts are complete and up to date and address the extent of backup and recovery services and each agency's responsibilities and priorities for restoring operations. Policies and procedures should specify the systems and data, if any, agencies would need to provide the Data Center in the event recovery efforts are needed.
- Update its comprehensive list of agencies with which it contracts for IT services at least annually to ensure that the services provided, including any systems and data needed from each agency, are appropriately identified and agency systems are prioritized for recovery based on their relative importance. Information from this list should be included or summarized in the IT service contract, or contract revision if needs change, with 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 2017-06.

Agency Response: Concur

Agency: Department of Administration
Name of contact person and title: Ed Yeargain, Sr. Information Security Engineer
Anticipated completion date: October 1, 2018
Agency's response: Concur

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

2018-04
Department of Child Safety—duplicate revenue transactions recorded

Condition and context— The Department of Child Safety (DCS) did not have adequate internal controls for recording and reconciling its intergovernmental revenues and receivables, and, therefore, did not detect and eliminate duplicate transactions recorded in the accounting system for fiscal years 2017 and 2018. During the year, the State's General Accounting Office discovered the errors and determined that intergovernmental revenues and receivables were overstated by $55.8 million and $137.2 million for fiscal years 2017 and 2018, respectively.

Criteria— DCS should establish and maintain effective internal control policies and procedures for recording and reconciling its intergovernmental revenues and receivables to help ensure that they are properly reported in the State's financial statements.

Effect— There is an increased risk that the State's financial statements could contain misstatements that are not prevented, or detected and corrected if DCS does not have adequate policies and procedures for recording and reconciling its intergovernmental revenues and receivables. The State's financial statements for the year ended June 30, 2018, reflect adjustments to correct these errors.

Cause— DCS has not determined how to prevent the duplicate transactions from occurring. Also, DCS did not eliminate duplicate revenue and receivable transactions that were automatically generated by the accounting system because it lacked enough employees to perform the reconciliations to identify which transactions should be eliminated.

Recommendations— DCS should either follow the State's policies and procedures for intergovernmental revenues or develop and implement its own written policies and procedures for recording and reconciling its intergovernmental revenues and receivables to prevent, or detect and correct, duplicate transactions. Policies and procedures should require a DCS employee to reconcile intergovernmental revenues and receivables recorded in the accounting system to detailed accounting records at least monthly and verify that any duplicate transactions are eliminated. Also, a second employee should review and approve the reconciliations.

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:

Agency: Department of Child Safety
Name of contact person and title: Ana Costache, DCS Finance Manager
Anticipated completion date: April 2019
Agency's response: Concur

In November 2018, the Department established a thorough and effective manual process for recording federal revenue. With the new process, all duplicate system automated revenue transactions are being discarded on a weekly basis.

The Department will create a desk procedure in an effort to better sustain this process by April 2019.

2018-05
Department of Revenue (DOR)—processing income tax revenues

Condition and context— The Department of Revenue (DOR) did not perform necessary reviews to ensure all of the State's income taxes were collected and reported in the State's financial statements.

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 tax revenue that is due. Also, the State may not report accurate income tax revenue in its financial statements.

Cause— DOR's information system did not have the functionality to perform automatic system checks and reconciliations, and DOR did not perform manual compensating review procedures to help ensure all income taxes are collected and reported in the State's financial statements.

Recommendation— To help ensure DOR is collecting and reporting all the State's income taxes, it should address its system's limitations or immediately implement alternative procedures to ensure necessary reviews are completed.

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 2017-10.

Agency Response: Concur

Agency: Department of Revenue
Name of contact person and title: Nicole Pope, Chief Internal Auditor
Anticipated completion date: June 30, 2020
Agency's response: Concur

The Department is in the planning phase of a project that will strengthen procedures for processing income tax revenues. The project is in the planning and requirements gathering stage. The project will be ran through the Department's governance process with an estimated completion date by the end of fiscal year 2020.

2018-06
Department of Insurance—reporting estimated liabilities associated with insolvent insurance carrier loss

Condition and context— The Department of Insurance (DOI) understated estimated liabilities associated with insolvent insurance carrier losses by $113.1 million for the year ended June 30, 2017. During fiscal year Arizona Auditor General State of Arizona—Schedule of Findings and Questioned Costs | Year Ended June 30, 2018 PAGE 15 2017, DOI was notified that 2 affiliated insurance carriers were declared as insolvent and that the DOI's Life and Disability Insurance Guaranty Fund would be required to pay the estimated costs associated with the 2,990 outstanding policies held by Arizona residents. However, when DOI provided the insolvency information to the Arizona Department of Administration's General Accounting Office (GAO) for reporting the liabilities in the State's June 30, 2017, financial statements, it included only the current portion of the loss and not the estimated long-term portion. As a result of this omission, the State's other enterprise funds' beginning net position for fiscal year ended June 30, 2018, was adjusted and decreased by $113.1 million to correct this error.

Criteria— U.S. generally accepted accounting principles (GAAP) require a liability to be recorded and disclosed for unpaid claims costs if it is probable that a loss has been incurred and the amount can be reasonably estimated.

Effect— The State's financial statements for the year ended June 30, 2018, reflect adjustments to correct the prior year's error. However, there is an increased risk that the State's financial statements could contain misstatements that are not prevented, or detected and corrected, if DOI does not provide all required information to GAO for the State's financial statements.

Cause— DOI did not include the full amount of estimated liabilities in the information provided to GAO in fiscal year 2017 because of staff oversight.

Recommendations— To help ensure the State's financial statements are presented in accordance with GAAP and are free from material misstatement, DOI should follow its established policies and procedures for providing information to GAO that is reported in the State's financial statements, including all necessary information for reporting estimated liabilities resulting from an insolvent insurance carrier loss.

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 Insurance
Name of contact persons and titles: Michael Surguine, Executive Director, Guaranty Funds
Anticipated completion date: Completed September 20, 2018
Agency's response: Concur

Arizona Life and Disability Insurance Guaranty Fund will make certain that the best estimates of the total liabilities for each insolvent insurer are included in its future financial statements by following its established policies and procedures and by having a person not involved in the preparation of the financial statements review them prior to submission to the General Accounting Office.

2018-07
Managing risk at Northern Arizona University

Condition and context— Northern Arizona University's (NAU) process for managing its risks did not include an adequate University-wide information technology (IT) risk assessment to respond to University-wide 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 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 NAU were impacted by disasters or other system interruptions.

Criteria—Effectively managing risk at NAU includes an entity-wide risk-assessment process that involves members of NAU's administration and IT management to determine the risks NAU 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 NAU might be subjected. To help ensure NAU's objectives can be met, an annual risk assessment should include considering IT risks. For each identified risk, NAU should analyze the identified risk and develop a plan to respond within the context of NAU'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 Arizona Auditor General State of Arizona—Schedule of Findings and Questioned Costs | Year Ended June 30, 2018 PAGE 16 information and the risk of losing the continuity of business operations in the event of a disaster or system interruption.

Effect— NAU's operations and IT systems and data may be susceptible to unintended and unnecessary risk.

Cause— NAU relied on an informal process to manage IT risks. Also, although NAU had developed written data classification procedures and had begun the process of inventorying its sensitive data, an entity-wide inventory had not been completed as of fiscal year-end.

Recommendations— NAU should identify, analyze, and reduce risks to help prevent undesirable incidents and outcomes that could impact business functions and IT systems and data. It also should plan for where resources should be allocated and where critical controls should be implemented. To help ensure it has effective entity-wide policies and procedures to achieve these objectives, NAU should follow guidance from a credible IT security framework such as that developed by 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 NAU's process for managing risk. NAU should conduct the following as part of its process for managing risk:

- Perform an annual University-wide IT risk-assessment process that includes evaluating risks such as risks of 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 inventorying the information NAU holds to assess where stronger access and security controls may be needed to protect data in accordance with State statutes and federal regulations.
- Evaluate and determine the business functions and IT systems that would need to be restored quickly given the potential impact disasters or other IT system interruptions could have on critical organizational functions, such as student services, and operations, such as payroll and accounting, and determine how to prioritize and plan for recovery.

NAU'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 NAU's separately issued report on internal control and on compliance for the year ended June 30, 2018, as finding 2018-01.

This finding is similar to prior-year finding 2017-12. NAU addressed some of the prior-year reported deficiencies by implementing a portion of the recommendations, and those are not included in this finding.

Agency Response: Concur

Agency: Northern Arizona University
Contact Persons:

Steve Burrell, Chief Information Officer
Michael Zimmer, Director of Information Security
Anticipated completion date: March 2019

Corrective Action Plan:
NAU has developed and implemented a University-wide, Enterprise Risk Management process that includes evaluating risks associated with IT. This was adopted in Spring 2018 and continued throughout 2018, including a more specific IT Risk Assessment completed in September and October 2018. An Information Security Policy and related Information Technology Risk Assessment standard were published in the University Policy Library in July 2018. A University Risk Committee has met to review these items on a regular basis and will continue to do so. This Committee includes IT representatives to ensure that IT risks are considered and evaluated.

NAU completed the development and implementation of a Data Classification and Handling Policy and set of Data Handling Protocols. The policy and protocols were published February 13, 2018 and revised July 2, 2018. They are published in the University Policy Library. An initial phase 1 of a Data Inventory took place in June and July 2018 with survey results gathered to inform the phase 2 in-depth Data Inventory planned to occur in the first quarter of 2019.

2018-08
Northern Arizona University (NAU)—Information technology (IT) controls—access, configuration management, security and contingency planning

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

- Restricting access to its IT systems and data—Procedures did not consistently help prevent or detect unauthorized or inappropriate access.
- Configuring systems securely—Procedures did not ensure IT systems were securely configured and configuration changes were adequately managed.
- Securing systems and data—IT security procedures lacked controls to prevent unauthorized or inappropriate access or use, manipulation, damage, or loss.
- Updating a contingency plan—Plan lacked key elements related to restoring operations in the event of a disaster or other system interruption

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

- Logical access controls— to ensure systems and data are accessed by users who have a need, access granted to systems and data is appropriate, and NAU monitors and reviews access to key systems and data..
- Well-defined documented configuration management process—Ensures NAU's IT systems are configured securely and that configuration changes are documented. This helps limit the possibility of an adverse impact on the system security or operations.
- 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— There is an increased risk that NAU may not adequately protect its IT systems and data, which could result in unauthorized or inappropriate access and the loss of confidentiality and integrity of systems and data. It also increases NAU'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— NAU had not revised its policies and procedures to ensure they adequately restricted access to its IT resources and relied on an informal configuration management process. Additionally, NAU made significant changes to its IT security policies and procedures and contingency plan but did not have time to fully implement these changes during the fiscal year.

Recommendations— To help ensure NAU has effective policies and procedures over its IT systems and data, NAU should follow guidance from a credible IT security framework such as that developed by the National Institute of Standards and Technology. To help

achieve these control objectives, NAU should develop, document, and implement control procedures in each IT control area described below:

Access

- Review employee user access ensuring appropriateness and compatibility with job responsibilities.
- Evaluate the use and appropriateness of accounts shared by 2 or more users and manage the credentials for such accounts.
- Manage employee-owned and entity-owned electronic devices connecting to NAU's systems and data.

Configuration management

- Configure IT resources appropriately and securely, manage configuration changes, and maintain configuration settings.
- Manage software installed on employee computer workstations.

Security

- Perform proactive key user and system activity logging and log monitoring, particularly for users with administrative access privileges.
- Prepare and implement a security-incident-response plan making it clear how incidents should be reported and handled.
- Perform IT vulnerability scans and remediate vulnerabilities in accordance with a remediation plan.

Contingency planning

- Update a contingency plan and ensure it includes all required elements to restore critical operations, including being prepared to enable moving critical operations to a separate alternative site if necessary.
- Test the contingency plan.
- Train staff responsible for implementing the contingency plan.

NAU'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 NAU's separately issued report on internal control and on compliance for the year ended June 30, 2018, as finding 2018-02.

This finding includes portions of similar prior-year findings 2017-13 (access), 2017-14 (configuration management), 2017-15 (IT security), and 2017-16 (contingency planning). NAU addressed some of the prior-year reported deficiencies by implementing some of the recommendations, and those are not included in this finding.

Agency Response: Concur

Agency: Northern Arizona University
Contact Persons:
Steve Burrell, Chief Information Officer
Michael Zimmer, Director of Information Security
Anticipated completion date: March 2019

NAU has implemented multi-factor authentication for higher risk areas and for users where job responsibilities include handling or processing of sensitive data types. NAU is continuing to implement multi-factor authentication through Q1 and Q2 of 2019 by evaluating other moderate to high risk areas first. NAU is drafting new policies, standards, and procedures for Access Controls, which will include periodic review of user access to ensure appropriate access levels to job responsibilities and the use of shared accounts.

NAU is currently revising, developing, and implementing configuration management policies and procedures that will include managing baseline configurations and changes made to those baselines, services and software, for servers and endpoints.

NAU has completed the development and implementation of an Information Security Policy and related Information Security Standards including an Auditing, Logging, and Monitoring Standard and a Vulnerability Management Standard. The policy and standards were published July 11, 2018 in the University Policy Library and include the recommendations provided.

NAU has completed the development and implementation of an Information Technology Incident Management policy and procedure. The policy and procedure were published in the University Policy Library October 18, 2018. Formal training and testing of the procedures are estimated to be implemented in Q1 2019 in alignment with the contingency plan listed below.

NAU is revising and updating its IT contingency plan which will include elements to restore critical operations, including IT operations, and preparation to enable the move of critical operations to an alternative location if necessary. The plan will involve training and frequent testing in 2019.

2018-09
University of Arizona (UA)—Managing risk

Condition and context— The University of Arizona's (UA) process for managing 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.

Criteria— Effectively managing risk at UA includes an entity-wide risk-assessment process that involves members of UA's administration and IT management to determine the risks 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 UA might be subjected. To help ensure UA's objectives can be met, an annual risk assessment should include consideration of IT risks. For each identified risk, UA should analyze the risk and develop a plan to respond to the risk within the context of UA's defined objectives and risk tolerances.

Effect— UA's administration and IT management may put UA's operations and IT systems and data at unintended and unnecessary risk.

Cause— UA had not fully developed or implemented its new comprehensive risk assessment process.

Recommendations— UA should identify, analyze, and reduce risks to help prevent undesirable incidents and outcomes that could impact business functions and IT systems and data. It also should plan for where resources should be allocated and where critical controls should be implemented. To help ensure it has Arizona Auditor General State of Arizona—Schedule of Findings and Questioned Costs | Year Ended June 30, 2018 PAGE 19 effective entity-wide policies and procedures to achieve these objectives, UA should follow guidance from a credible IT security framework such as that developed by the National Institute of Standards and Technology. Also, UA should perform an annual entity-wide IT risk-assessment process that includes evaluating risks, such as risks of inappropriate access that would affect financial data, system changes that could adversely impact or disrupt system operations, and inadequate or outdated system security.

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 UA's separately issued report on internal control and on compliance for the year ended June 30, 2018, as finding 2018-01.

This finding is similar to prior-year finding 2017-18.

Agency's Response: Concur

Agency: University of Arizona
Contact Person: Lanita Collette, Chief Information Security Officer
Anticipated Completion Date: June 2019

The University acknowledges that our IT risk assessment process needs additional work.

A thorough review of risk assessment needs for revising and expanding the current risk assessment process revealed that the use of professional services to complete risk assessments would exceed available budget and would require cost prohibitive annual re-

assessments. As an alternative, a plan was developed to identify and provide professional training to risk managers, so they can complete the necessary assessments at a lower cost to the University.

To prepare for the first risk assessment cycle, the Information Security Office (ISO) acquired, installed, and configured software tools to enable inventory of resources and risk assessment. These tools provide central tracking and enable enforcement of completion. Training on properly completing and reporting on risk assessments will be conducted in November and December of 2018. Once risk assessments are completed, risk managers will be guided by the ISO to create security remediation plans guided by our risk-based approach. Revised policies governing enforcement were completed by June 30, 2018 and are pending University leadership final approval.

2018-10
University of Arizona Information technology (IT) controls—access, security, and contingency planning

Condition and context— The University of Arizona's (UA) IT control procedures were not always sufficiently designed, documented, and implemented to respond to risks associated with its IT systems and data. Further, UA did not clearly designate oversight and monitoring responsibilities to ensure that its business units followed University-wide IT policies and procedures. UA lacked adequate procedures over the following:

- Restricting access to its IT systems and data—Policies and procedures did not include logging and monitoring users with elevated access to UA's enterprise systems.
- Securing systems and data—IT security policies and procedures lacked controls to prevent unauthorized or inappropriate access or use, manipulation, damage, or loss. Further, procedures did not include identifying, classifying, and inventorying sensitive information that might need stronger access and security controls.
- Developing and documenting a contingency plan—UA lacked a plan for restoring operations in the event of a disaster or other system interruption. Further, UA did not identify the business functions and IT systems that would need to be restored quickly if UA were impacted by disasters or other system interruptions.

Criteria— UA should have effective internal controls to protect its IT systems and help ensure the integrity and accuracy of the data it maintains. Further, effective oversight and ongoing monitoring activities are crucial for UA to assess the effectiveness of its IT policies and procedures and take necessary remedial action.

- Logical access controls—Help to ensure systems and data are accessed by users who have a need, access granted to systems and data is appropriate, and UA monitors and reviews access to key systems and data.
- 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—There is an increased risk that UA may not adequately protect its IT systems and data, which could result in unauthorized or inappropriate access and the loss of confidentiality and integrity of systems and data. It also increases 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— UA had not completed its process of assigning oversight and monitoring responsibilities for decentralized IT internal controls. In addition, policies and procedures for access, data classification, and security were either still under development, awaiting approval, or not fully implemented. In addition, UA did not perform a business impact analysis because it had not completed its disaster recovery procedures to align with the movement of its enterprise systems into a cloud environment.

Recommendations— To help ensure UA has effective policies and procedures over its IT systems and data, UA should follow guidance from a credible IT security framework such as that developed by the National Institute of Standards and Technology. Further, UA should clearly designate oversight and perform ongoing monitoring activities to ensure its business units follow University-wide IT policies and procedures. To help achieve these objectives, UA should develop, document, and implement control procedures in each IT control area described below:

Access

- Monitor and review key activity of users with elevated access to its enterprise systems.

Security

- Improve IT vulnerability scans and remediate vulnerabilities in accordance with a remediation plan.
- Identify, evaluate, and apply patches in a timely manner.
- Develop, document, and follow a process for awarding IT vendor contracts.
- Implement existing policies for identifying, classifying, inventorying, and protecting sensitive information UA holds to assess where stronger access and security controls may be needed to protect data in accordance with State statutes and federal regulations.

Contingency planning

- Evaluate and determine the business functions and IT systems that would need to be restored quickly given the potential impact disasters or other IT system interruptions could have on critical organizational functions, such as student services, and operations, such as payroll and accounting, and determine how to prioritize and plan for recovery.
- Develop and implement a contingency plan and ensure it includes all required elements to restore critical operations.
- Test the contingency plan.
- Train staff responsible for implementing the contingency plan.
- Test backups of systems and data.

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 UA's separately issued report on internal control and on compliance for the year ended June 30, 2018, as finding 2018-02.

This finding is similar to prior-year findings 2017-17 (oversight), 2017-18 (risk assessment), 2017-19 (access), 2017-20 (security), and 2017-21 (contingency planning).

Agency Response: Concur

Agency: University of Arizona
Contact Person: Lanita Collette, Chief Information Security Officer
Anticipated Completion Date: June 2019

Oversight and monitoring:
The University acknowledges that oversight of technical controls in our distributed computing environment needs improvement. To address this need, the Information Security Office 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.

Security tools have been deployed to monitor internet and internal network traffic, block known malicious activity, and alert on suspicious activity. The University contracted with a vendor for security operation services to monitor alerts 24/7.

By June 30, 2018, the information security office had grown from two to ten staff members and staff began updating policies, including a policy to address enforcement of required security practices. These policies will be presented to campus leadership in December of 2018 for approval. Staff were also able to deploy a solution for tracking inventory in preparation for risk assessment training in November and December 2018. All campus units are required to participate in the inventory, to be enforced by the Information Security Office (ISO) supported by departmental leadership, as directed by policy.

Several playbooks were developed and distributed to IT staff to aid in consistent and informed response to information security incidents. Additionally, a security Special Interest Group was formed that has membership from all major campus units. This group enhances information sharing about new solutions released by the ISO and ensures that campus units understand new requirements in proposed policies.

Restricting access to its IT systems and data:
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.

The University has produced a draft access control policy, purchased and installed a logging and monitoring solution and was in the process of testing and preparing to ingest log data. Processes and procedures for privileged access management are still under development and may require the acquisition of additional software or services.

Developing and documenting a contingency plan:
The University has revised and tested its backup procedures to align with the movement of enterprise web applications to cloud services. Procedures are documented and a draft policy has been created. 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. The University will move forward to address business impacts by identifying critical IT systems that will need to be restored quickly in the event of disruption.

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. Documenting of procedures is an on-going effort.

Staff education on the process has also been an on-going effort. Key personnel who are directly involved in the configuration have learned the process. Staff generally have been made aware that the process is now automated within our cloud service. In addition, as of October 2018 we have documented the steps and successfully completed a disaster recovery exercise around our Financial application.